hors-série

svm

LES GRANDS DOSSIERS

Collection SVM Les Grands Dossiers n° 2

LES MAFIAS ATTAQUENT LE WEB

ESPIONNAGE, VOL DE DONNÉES, RACKET...

Le cri d'alarme des experts

Les parades pour l'internaute

Volnay

Belgique : 4,50 € • Suisse : 8 CHF

T 04277 - 30 H - F: 3,90 € - RD

www.svmlemag.fr

KASPERSKY lab

« Parce qu'on ne joue pas avec la sécurité! »

Versions 2009

Protection étendue
- Un nouveau pare-feu de niveau professionnel
- Réseaux Wi-Fi et VPN sécurisés Nouveau !
- Classement en fonction du niveau de danger potentiel des applications connues et inconnues : module HIPS (Host intrusion prevention systems) Nouveau !
- Système de prévention des attaques de réseaux (IPS)

Protection préventive
- Analyse complète du système d'exploitation et des applications Nouveau !
- Désactivation des liens vers les sites infectés de malwares Nouveau !
- Surveillance préventive (Kaspersky® Security Network) Nouveau !

© 2008. Kaspersky Lab France. Tous droits réservés. Retrouvez l'ensemble de la gamme Kaspersky Lab sur www.kaspersky.fr

hors-série svm LES GRANDS DOSSIERS www.svmlemag.fr

Publié par Volnay Publication France – 34, rue Jean-Jaurès 92800 Puteaux
✆ 01 46 92 54 00 – Fax : 01 46 92 54 01
Fax rédaction : 01 46 92 54 05 (pour joindre directement votre correspondant, composez le 01 46 92 suivi de son numéro de poste)

RÉDACTION
Rédaction en chef Delphine Sabattier
Rédaction en chef déléguée Éric Le Bourlout
Rédaction Ludovic Dupin, Nicolas Robaux
Secrétariat général de rédaction Rémi Gancel
Conception graphique et maquette Thierry Laurent

ONT COLLABORÉ À CE NUMÉRO
Jacques Harbonn, Bruno Mathé, Nicolas Reynaud

Photographies et illustrations
AP/Sipa/Sauday Alamba, Sipa/Baziz Chibane, LPC gendarme Philippe Latrubesse, Sipa/Pouzet/20 minutes
Couverture Thierry Laurent (conception graphique)

Assistante de rédaction Corinne Coat (5510) – fax : 01 46 92 54 05

SITES WEB MAGAZINES
François Dupin **Rédacteur en chef technique**
Moudar Akbaraly **Développeur webmestre**
François Fouquet **Assistant webmestre**

DIRECTION
Jacques Lefranc **Président**

PUBLICITÉ
Christelle Pasquier **Directrice commerciale SVM, SVM Mac, PC Expert, www.SVMlemag.fr** (5430)
Valérie Atlani **Directrice de clientèle** (5431)
Julien Barbey **Chef de publicité** (5433)
Assistante commerciale et technique (5432)

MARKETING
Jeanne-Marie Seurbier **Responsable marketing et études** (5440)

DIFFUSION
Guillaume Plassais **Responsable des diffusions** (réservé aux dépositaires de presse : 5445)
Laure Rousseau **Assistante de diffusion** (5447)
Marina Vérité **Responsable administrative de la diffusion** (5446)

Service abonnements et commandes d'anciens numéros
✆ **01 44 84 80 26** ; fax : 01 42 00 56 92 ; SVM, 18-24, quai de la Marne 75164 Paris Cedex 19, e-mail : svmabo@dipinfo.fr ; heures d'ouverture : de 8 h à 18 h du lundi au vendredi sans interruption. Pour nos abonnés suisses, merci de bien vouloir contacter notre service abonnement à l'adresse suivante : Dynapresse Marketing SA, 38 av. Vibert, CH 1227 Carouge ✆ 2022 308 08 08 ; fax 022 308 08 59 ; e-mail abonnements@dynapresse.ch Pour la Belgique, éditeur responsable : Ediglroup Sprl Bastion Tower Etage 20, place du Champ-de-Mars 1050 Bruxelles ; tél. : 070 233 304, fax : 070 233 414, adobelgique@edigroup.org.

INFORMATIQUE ET PRODUCTION
Frédéric Pognant **Responsable Informatique** (5455)
Frédéric Lévesque **Responsable Production**
Vincent Hermouet **Technicien informatique** (5456)

LABORATOIRE ET TESTS
Lionel Morillon **Responsable Laboratoire**
Cyril Duffez et Lauwiks Cutman **Rédacteurs-testeurs**

Volnay PUBLICATION FRANCE

OJD PRESSE PAYANTE 2005

Capital social : 7 308 260 €. RCS Paris 494 16566500030
© 1995 Science et Vie Micro.
Dépôt légal décembre 1997. ISSN 1634-4265X. Siège social : 34, rue Jean-Jaurès 92800 Puteaux. Directeur de publication : Jacques Lefranc. Imprimerie Dulac Media Partenaire, Route de Paris, 27120 Pacy-sur-Eure. Commission paritaire n° 0313K85514. Imprimé en France. Ce hors-série comporte un encart abonnement SVM jeté. Abonnement SVM format classique 11 nos France 38 €, format Pocket 11 nos 25 €. Pour les autres pays, merci de nous consulter au 01 44 84 80 26.

Bons baisers de Russie

Cela n'a pris que quelques secondes. Je reçois un spam avec pour seul texte un fichier exécutable… Un clic, et boum ! Mon vaillant PC est devenu la victime d'une énième variante de Zlob, un cheval de Troie en mutation permanente, qui pollue le Web depuis plus de deux ans. Et mon antivirus, que faisait-il ? Bah… Il n'a rien vu du tout.

Cette fois, j'ai contaminé mon ordinateur volontairement, pour les besoins de la cause. Mais Zlob, ou des milliers de virus plus modernes, empoisonnent chaque jour de nouveaux internautes, souvent sans même qu'ils s'en aperçoivent. En douce, ils transforment leur ordinateur en pantin au sein d'un botnet, ces réseaux de PC zombies, loués par les pirates à d'autres escrocs pour envoyer des pourriels, des spams ou de nouveaux virus. Fini le temps où la création de virus était l'apanage des "nerds" en mal de défi technique. Désormais, les cybercriminels mènent la danse. Nombreux et motivés, ils en veulent à vos données personnelles et au final à votre argent : le Zlob que j'ai attrapé me proposait d'acheter un faux antivirus pour me débarrasser de lui, avant de planter ma machine. Un autre virus qui vient de débarquer crypte votre disque dur grâce à une clé de 1 024 bits… Il vous propose ensuite de récupérer vos données en achetant, très cher, un décrypteur.

Comme bien des virus actuels Zlob est d'origine russe : il a peut-être été conçu par ce qui est considéré comme la plus importante cybermafia au monde : le Russian Business Network. Une pieuvre qui trempe ses tentacules dans tout ce que le Web compte de plus louche. Le RBN a créé Mpack – une suite d'outils qui infecte des sites Web et installe un keylogger chez ceux qui les visitent –, qu'il vend en sous-main pour la coquette somme de 1000 $. Il est aussi à l'origine du virus et du botnet Storm, qui ont déjà contaminé plusieurs centaines de milliers de machines.

Dans ce hors-série, nous vous proposons une plongée dans l'univers inquiétant et fascinant de la cybercriminalité. Depuis ses origines, la "belle époque" des premiers virus et du phreaking cher à Captain Crunch, jusqu'aux escrocs qui aujourd'hui tentent de vous extorquer de l'argent et prendre le contrôle de votre PC. Vous verrez aussi comment la riposte s'organise, grâce aux témoignages des plus grands experts en sécurité informatique, et de quelle façon vous pouvez vous défendre face à ces mafias qui investissent la Toile chaque jour un peu plus.

ÉRIC LE BOURLOUT

Les mafias attaquent

6 LE THÉÂTRE DU CRIME

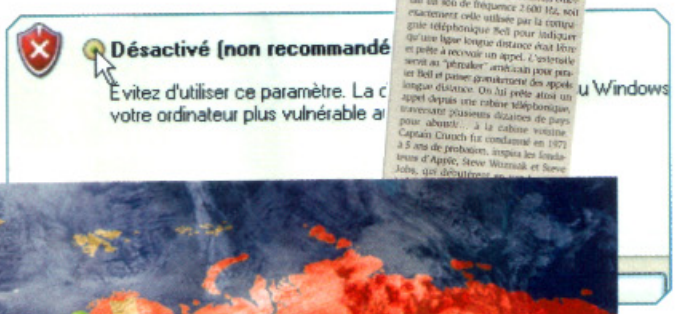
Qui sont-ils, où sont-ils, que font-ils ? Nous levons un coin du voile sur le monde parallèle et protéiforme des hackers.

6 Un monde de cyberbandits
8 Quoi de neuf sur le front ?
10 La grande histoire des virus
14 Princes des hackers : le côté obscur du génie
16 Internet est-il assez solide ?

18 LES MENACES

Depuis les premiers vers croqueurs de disque dur, le pouvoir de nuisance des "malwares" a beaucoup évolué. Et pas vraiment dans le bon sens.

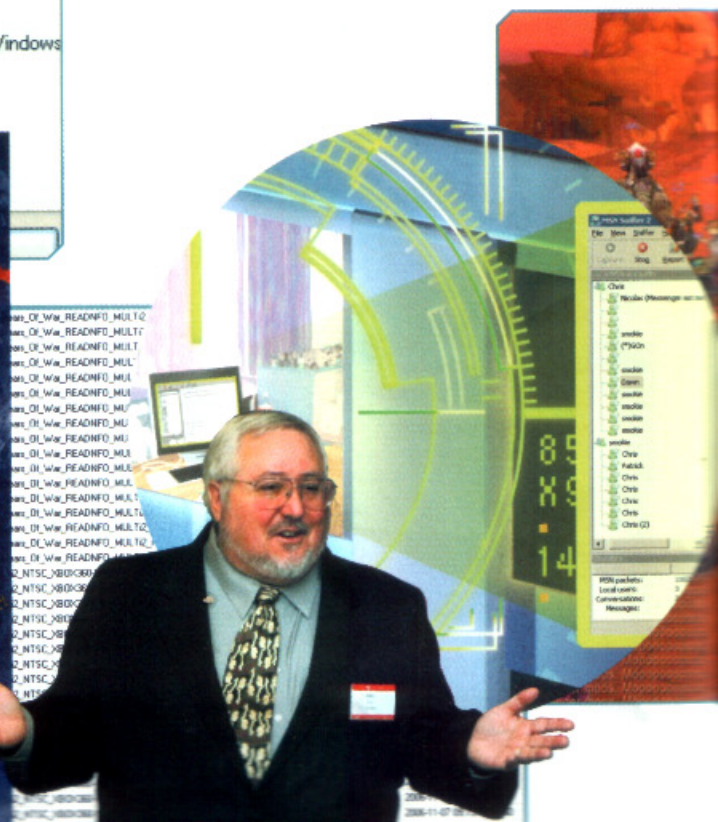
18 Les pirates fondent sur les communautés
20 Le Web 2.0, un village où tout se sait
22 Phishing : gare aux requins de l'e-mail !
24 Scam : les virtuoses de la corde sensible
27 Spam : un vieux casse-pieds toujours vert
28 Les entreprises : un proie trop facile ?
30 Ce que vos collègues savent sur vous
32 Qui se cache derrière les contenus illicites ?
35 Gare aux contrefaçons !
36 Attention, cyberguerre en vue



Il siphonne Bell avec un sifflet pour enfants

John T. Draper

Plus connu sous le surnom de Captain Crunch, qu'il doit aux boîtes de céréales Cap'n Crunch, vendues à la fin des années 60 avec un petit sifflet pour enfants. Lequel sifflet, découvrirent John T. Draper et son ami Joe Engressia (alias Joybubbles), émettait un son de fréquence 2 600 Hz, soit exactement celle utilisée par la centrale téléphonique Bell pour indiquer qu'une ligne longue distance était libre et prête à recevoir un appel. L'ex-ennemi serait un "phreaker" américain pour pirater Bell et passer gratuitement des appels longue distance. On lui prête alors un appel depuis une cabine téléphonique, traversant plusieurs dizaines de pays pour aboutir... à la cabine voisine. Captain Crunch fut condamné en 1971 à 5 ans de probation, inspira les fondateurs d'Apple, Steve Wozniak et Steve Jobs, qui débutèrent en



le Web

LE CASSE VIRTUEL DU SIÈCLE

Le casse virtuel du siècle : c'est ce qu'a fait réussir le Russe Vladimir Levin en 1994. Il pratique alors le système informatique de la banque Citibank, accède à plusieurs comptes d'entreprises et fait virer 10,7 millions de dollars vers cinq comptes à l'étranger. Mais trois de ses complices sont arrêtés à Tel Aviv, San Francisco et Rotterdam lorsqu'ils tentent de retirer les fonds. Condondu, Levin est protégé par l'absence de traité d'extradition entre la Russie et les États-Unis. Cependant, une escale à Londres lui sera fatale : il est arrêté, en mars 1995, par Scotland Yard. Après une intense bataille juridique, il sera finalement jugé en février 1998 aux États-Unis et condamné à 3 ans de prison. Bien plus tard, en 2005, un hacker russe prétendra que Levin s'était, à l'époque du casse, contenté d'acheter pour 100 $ une porte dérobée du système de Citibank.

38 LEUR MÉTIER : VOUS PROTÉGER

En amont ou en aval, sur les réseaux ou au sein de votre PC, ils ont déclaré la guerre aux pirates. Mais en ont-ils les moyens ?

38 Du renfort pour la police du Net
42 Les pédophiles pris dans la Toile
44 Sur les lieux du crime, place à l'expert
48 Logiciels de sécurité : jusqu'où protègent-ils ?
52 Pour/contre : doit-on compter sur les antivirus ?

54 VIGILANCE CITOYENNE

Sans votre coopération, la lutte contre le mal se réduit à néant. Apprenez à vous défendre pour que le hacking ne passe plus par vous.

54 Un pare-feu gratuit pour se réfugier dans ses murs
56 Le contre-espionnage, c'est votre affaire aussi !
57 Des sites pour prendre le dessus
58 Facebook : 10 règles pour se faire respecter
60 Self-defense : l'antivirus ne le fait pas pour vous

62 À VOIR, À SAVOIR

62 Culture pirate – *des films, des livres*
64 Le meilleur du spam et du scam – *pour rire* ☺
66 Quiz – *êtes-vous bien informé ?*

Un monde de cyber

***Fini, les Robins des Bois** assoiffés de gloriole du Net pionnier, place aux mafias avides de profits du Web marchand !*

Internet abolit les frontières pour le meilleur mais aussi le pire. Comme l'économie, la cybercriminalité s'est mondialisée. Désormais, les escrocs peuvent opérer à l'échelle de la planète, lancer des attaques depuis n'importe quel pays. Deux tiers des affaires traitées par les services spécialisés de police et de gendarmerie finissent à l'étranger. Les enquêteurs ont du mal à remonter aux instigateurs. La coopération judiciaire n'est pas toujours très efficace et les malfaiteurs du Web s'emploient à brouiller les pistes en multipliant les serveurs relais, les intermédiaires.

Des mafias internationales

Les réseaux mafieux ont supplanté les bidouilleurs de génie, la cybercriminalité s'est professionnalisée. Comme dans l'économie classique, on assiste à une division du travail. Les fournisseurs de malwares, les donneurs d'ordre et les exécutants sont rarement les mêmes personnes. Un cheval de Troie fabriqué en Europe de l'Est peut être acheté par une mafia russe et disséminé à partir d'un botnet contrôlé depuis les États-Unis. Dans ces conditions, difficile de dresser un tableau précis de la cybercriminalité, de savoir exactement qui fait quoi, d'où vient le ver ou le cheval de Troie débusqué sur son ordinateur. Les éditeurs de solutions de sécurité publient régulièrement des chiffres et des classements pour chaque type de menace. Les pourcentages avancés sont rarement concordants. Par contre, au fil des études et des enquêtes menées par les services spécialisés, les mêmes noms de pays reviennent depuis plusieurs années. Il est possible de dresser une carte, même approximative de la cybercriminalité. Il ne s'agit pas de stigmatiser les autorités des États cités mais bien de montrer que le phénomène ne pourra être endigué que grâce à une coopération renforcée entre les gouvernements et la mise en place d'outils transnationaux. • **N.Re.**

*** MALWARE**
Ce terme, contraction de "malicious" et de "software", désigne tout programme malveillant, qu'il s'agisse de virus, cheval de Troie, rootkits ou autre spyware.

BOTNET
Un botnet est un réseau de machines "zombies" constitué par des pirates pour perpétrer leurs forfaits (envoi de spam, phishing, etc.) Il est composé de PC d'internautes qui se sont fait contaminer par un cheval de Troie, et ignorent que leur machine sert des cybercriminels. Certains réunissent plus de 300 000 machines !

bandits

PRINCIPALES RÉGIONS D'ACTIVITÉ DE LA CYBERCRIMINALITÉ
ÉMISSION DE SCAMS
Afrique (Nigeria, Côte d'Ivoire, République démocratique du Congo, Sierra Leone, Ghana), Russie, Ukraine, Philippines.
RÉSEAUX DE PC ZOMBIES
Chine, États Unis, Europe occidentale, Inde, Japon, Océanie...
PRÉSENCE D'ORGANISATIONS MAFIEUSES PARTICULIÈREMENT ACTIVES DANS LA CYBERCRIMINALITÉ
Russie, Chine
FABRICATION DE MALWARES
Russie, Europe de l'Est (Ukraine, Roumanie, Bulgarie), Chine

QUOI DE NEUF SUR LE

anniversaire

Les 30 ans du Spam

"DIGITAL VA FAIRE UNE PRESENTATION PRODUIT DES NOUVEAUX MEMBRES DE LA FAMILLE DECSYSYEM-20"

3 Mai 1978

Un cadre de la société DEC envoie, ce jour-là, un message publicitaire vantant les capacités de nouveaux ordinateurs à 400 personnes de la côte ouest des Etats-Unis. Le Spam vient de naître sur Internet, qui s'appelle encore Arpanet à l'époque. Ce pourriel n'avait pourtant pas grand-chose a voir avec les envois de masse que l'on connaît aujourd'hui. L'individu avait du taper les 400 noms à la main… Un travail fou qui avait d'ailleurs dépassé les capacités techniques du logiciel qu'il avait employé, et la moitié des destinataires n'avaient du coup jamais reçu le message. Le premier spam avait, bien entendu, provoqué de vives réactions chez les "arpanautes" qui l'avaient reçu… *"Ceci est une violation flagrante de l'usage d'Arpanet, car le réseau ne doit être utilisé que pour les affaires officielles du gouvernement US. Une mesure appropriée est en train d'être prise pour empêcher que cela ne se reproduise"*, annonçait alors le major Raymond Czahor, responsable de l'Arpanet. Apparemment, les mesures n'ont pas suffi ! Quant au terme "spam", il vient d'un sketch des impayables Monty Python, dans lequel un couple tente de petit-déjeuner dans un restaurant. Mais tout ce que la patronne a à proposer, ce sont des plats à base de *"spam, spam, spam, spam, spam"*. Le terme, répété des dizaines de fois durant le sketch, aurait été assimilé à ces mails exaspérants qu'on reçoit eux aussi par dizaines…

java mobile

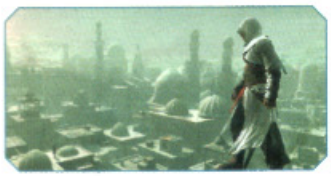
LES TÉLÉPHONES PORTABLES, NOUVELLES CIBLES DES HACKERS ?

Cela pourrait prêter à sourire, mais il semblerait bien que même nos téléphones portables, pourraient bientôt devenir des cibles de choix pour les pirates. Et pour cause : ils recèlent non seulement, des informations personnelles potentiellement utiles, mais peuvent être également utilisés à votre insu pour garnir les poches des pirates. Les virus les plus récents, heureusement encore peu répandus, arrivent sous la forme d'un programme Java (ils se font passer pour un jeu, par exemple) récupéré sur un site peu fiable… Sur certains téléphones, ils sont ensuite capable d'appeler en douce des numéros surtaxés. Les téléphones intelligents (Symbian ou Windows Mobile) sont encore plus sensibles aux malwares que les mobiles classiques, car on peut y installer facilement des programmes supplémentaires. Les labos de Kaspersky ont ainsi récemment découvert un nouveau cheval de Troie pour Windows Mobile, InfoJack.a. Il s'installe en même temps que Google Maps Mobile ou qu'un jeu et vole certaines informations, comme le numéro IMEI, les applications installées, etc., pour les envoyer au propriétaire du site qui avait mis programmes et virus en ligne.

crypter, c'est pas joué

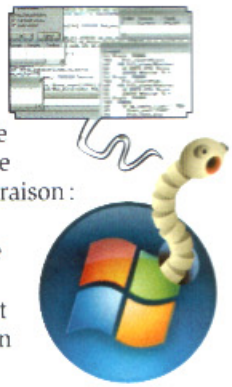
DES PUCES TPM CONTRE LE PIRATAGE DES JEUX PC ?

Les éditeurs de logiciels de jeux PC sont en guerre contre les teams pirates, qui crackent puis distribuent leurs jeux gratuitement sur Internet (*voir page 32*). Nolan Bushnell, le fondateur d'Atari croit connaître la solution : crypter les prochains jeux vidéos. Et ce grâce aux puces TPM, déjà présentes sur bien des PC professionnels, qui si elles se répandent dans les PC grand public pourraient – pourquoi pas – être obligatoires pour installer certains titres, à l'avenir. Ultime ? Pas sûr : tous les systèmes de cryptage mis en place pour protéger des contenus ont pour l'instant sauté les uns après les autres sous les coups de boutoir des hackers…



peut mieux faire

Vista, pas si sûr que ça



Microsoft a beaucoup vanté la sécurité améliorée de son nouveau système d'exploitation. Avec raison : son (incommodant) système UAC s'avère capable de stopper certains malwares, et son outil de détection de programmes malveillants fonctionne. Mais Vista est loin d'être exempt de virus. D'après une analyse de PC Tools basée sur les statistiques de son logiciel Threatfire, 27 % des machines des utilisateurs sous Vista auraient été victimes d'un programme malicieux.

FRONT ?

››› antihéros

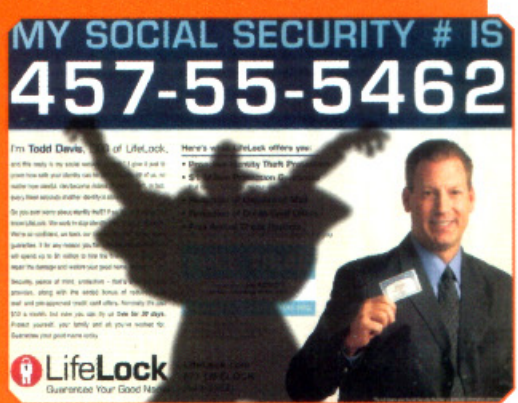
Vol de données massif au Chili

Il se fait appeler le "lâche anonyme" et a fait trembler le gouvernement du Chili. Ce hacker est en effet parvenu à pirater plusieurs serveurs officiels chiliens, appartenant à l'armée, aux services électoraux ou encore au ministère de l'Éducation. Et a volé les informations personnelles de… 6 millions de citoyens, avec noms et adresses, numéros de cartes d'identité et de téléphone, mails… Avant de poster le tout sur Internet. Bien qu'elles aient toutes été retirées, elles ont largement eu le temps d'être copiées et réutilisées au mieux par des spammeurs!

››› trop sûr… de lui

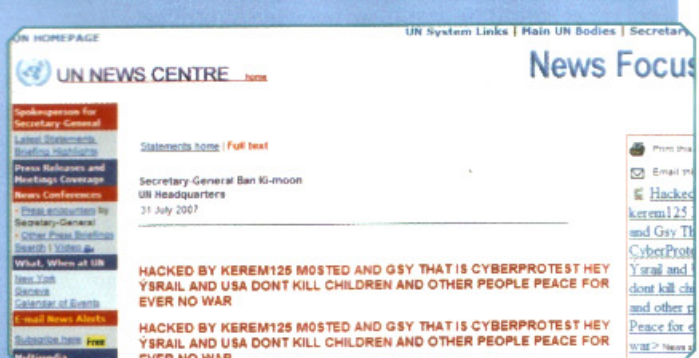
L'IDENTITÉ VOLÉE DU PROTECTEUR D'IDENTITÉ

C'est l'arroseur arrosé. Todd Davis était bien connu aux USA pour une publicité vantant son entreprise, LifeLock. Il y apparaissait souriant, avec à la main sa carte de sécurité sociale. Et n'hésitait pas à montrer à l'Amérique entière combien son service, censé protéger ses clients contre le vol d'identité, était sûr, en laissant clairement apparaître son numéro de sécu sur toutes ses pubs… Mais voilà, Todd David a été récemment victime d'un vol d'identité : grâce à son numéro largement diffusé, un inconnu s'est ouvert un compte en ligne avec un crédit de 500 $… L'affaire ne pouvait pas plus mal tomber pour M. Davis, alors qu'une "class action" (action juridique de groupe) s'ouvre contre son entreprise, accusée par certains clients de n'être qu'une vaste arnaque…



››› contagion

Les virus en ligne : une nouvelle plaie



Le Web est-il menacé par les pirates ? Le constat alarmant dévoilé par F-Secure fin avril, tendrait à le prouver. L'éditeur d'antivirus a déniché fin avril pas moins de 510 000 pages Web infectées par un code malicieux. Et pas des moindres : des sites gouvernementaux britanniques et plusieurs de l'ONU comptent parmi les sites piratés. Des sites qui, du coup, deviennent des réceptacles à virus, qu'ils peuvent ensuite transmettre aux internautes (sous Windows seulement !) qui les visitent. Le but du malware qui a été utilisé ici ? Rien moins que de dérober vos mots de passe… Cela fait froid dans le dos, d'autant que d'après F-secure, cette méthode de contamination ne fait que s'amplifier de semaine en semaine. D'après la société CheckPoint, qui édite les solutions Zone Alarm, 7 sites sur 10 seraient vulnérables à ce genre d'attaque. En fait, c'est une faille de la très populaire base de données SQL qui est exploitée dans ce cas : si le site est mal programmé, les pirates peuvent obtenir un accès administrateur à la base de données et injecter leur virus en ligne.

››› c'est arrivé près de chez vous

UN GANG DE HACKERS ARRÊTÉ EN FRANCE

La France a aussi ses hackers. La police a démantelé fin mai un réseau de 22 jeunes pirates âgés de 14 à 25 ans. Ils n'habitaient pas la même région mais se sont alliés pour pénétrer les systèmes informatiques de plusieurs sociétés françaises, russes ou islandaises… Sur lesquels ils ont détruit des fichiers clients, trafiqué des bases de données… Autre forfaits, plus graves : la création de sites de phishing pour récupérer des coordonnées bancaires. Ils risquent tous deux ans de prison et 30 000 euros d'amende.

La grande histoire des

C'est un vieux briscard de la sécurité informatique qui nous la raconte. *Voilà 25 ans que David Perry suit de très près le monde de la sécurité et l'évolution du malware. Aujourd'hui directeur global pour l'éducation chez l'éditeur d'antivirus Trend Micro, il parcourt le monde pour parler de sa passion. La saga des virus informatiques, il l'a vécue de l'intérieur, des premiers virus de boot au ver de réseau Melissa.*

témoignage

SVM : Quelles sont les origines des virus informatiques ?

David Perry : Les premiers virus ne sont pas apparus sur un logiciel ou un matériel informatique. Ils sont nés dans une œuvre de fiction, en fait un roman de John Brunner, appelé *Sur l'onde de Choc*. Les virus ont existé dans bien des œuvres de fiction avant d'apparaître en vrai. La plupart des idées que l'on se fait sur les hackers, les virus, les chevaux de Troie… nous viennent de la littérature et du cinéma. Prenez les films : les virus y sont toujours "visuellement dramatiques", ils créent une interface avec une pieuvre géante qui recouvre votre bureau, ils font exploser votre ordinateur, retournent un bateau pétrolier, ouvrent un coffre à la banque ou font débarquer les extraterrestres… Dans les films, ils sont immédiats et spectaculaires. Dans la réalité, évidemment, ce n'est pas la même chose. Le tout premier virus informatique pour ordinateur personnel a été écrit en 1982 pour l'Apple II par un gamin de 16 ans nommé Rich Skrenta. Il se surnommait Elk Cloner et ne créait aucun dommage à la machine : il se contentait d'écrire un poème sur l'écran de l'Apple II. Cela a fait grand bruit, car Elk Cloner est passé pour le premier programme "autorépliquant".

Ceci avait été théorisé la même année par un professeur nommé Fred Cohen, qui en a parlé dans son essai *Un cours sur les virus informatiques*. Il utilisa le terme "virus" pour qualifier les autoréplicants, mais pensait que le mot virus avait un trop grand impact émotionnel. Il avait plutôt envie d'appeler ces nouveaux programmes des "automates cellulaires autoréplicants", car les virus s'inspirent des automates cellulaires conceptualisés par le mathématicien hongrois John Von Neumann lorsqu'il posa les bases de *La théorie du jeu*. C'est exactement ce que sont les virus, des programmes écrits pour se répliquer tout seuls. Les virus n'ont donc pas forcément de visée destructrice, ils ne sont pas forcément mauvais, ces programmes ont juste besoin de faire des copies d'eux-mêmes, répondant ainsi à la définition d'un virus.

> *"LES FRÈRES ALVID ÉTAIENT SI FIERS D'AVOIR CRÉÉ LE PREMIER VIRUS QU'ILS L'AVAIENT SIGNÉ !*

Maintenant, je vais compliquer un peu plus les choses. En 1971 sur un supercalculateur de la compagnie BBN a été écrit le premier ver capable de se répandre sur le réseau : Creeper répondait à la définition du virus que nous venons d'évoquer, mais n'a pas eu le succès escompté : il s'est trouvé confiné à une seule machine et plus personne n'en a entendu parler. Le prix "premier virus pour ordinateur IBM PC" revient à deux frères de Lahore au Pakistan : Basit et Amjad Farooq Alvid, qui en 1986 écrivirent Brain. Il n'était pas destructif, il inscrivait simplement une pub pour leur magasin d'informatique sur votre écran… Et les deux frères étaient si fiers d'avoir inventé le premier virus PC qu'ils avaient intégré leur noms, adresse et numéro de téléphone dans le code du virus ! Brain a provoqué une vraie panique dans les médias américains, car la légende du virus destructeur était déjà bien ancrée. Ils ont réagi de façon excessive : *"C'est la fin du monde ! Débranchez vos ordinateurs !"*. Ils sont allé chercher Peter Norton, très connu à l'époque pour ses utilitaires pour PC, et lui ont demandé : *"Peter, que pensez-vous de ce virus ?"* Ce à quoi il a répondu

DAVID PERRY, une mine d'expérience et d'anecdotes croustillantes en matière de sécurité informatique.

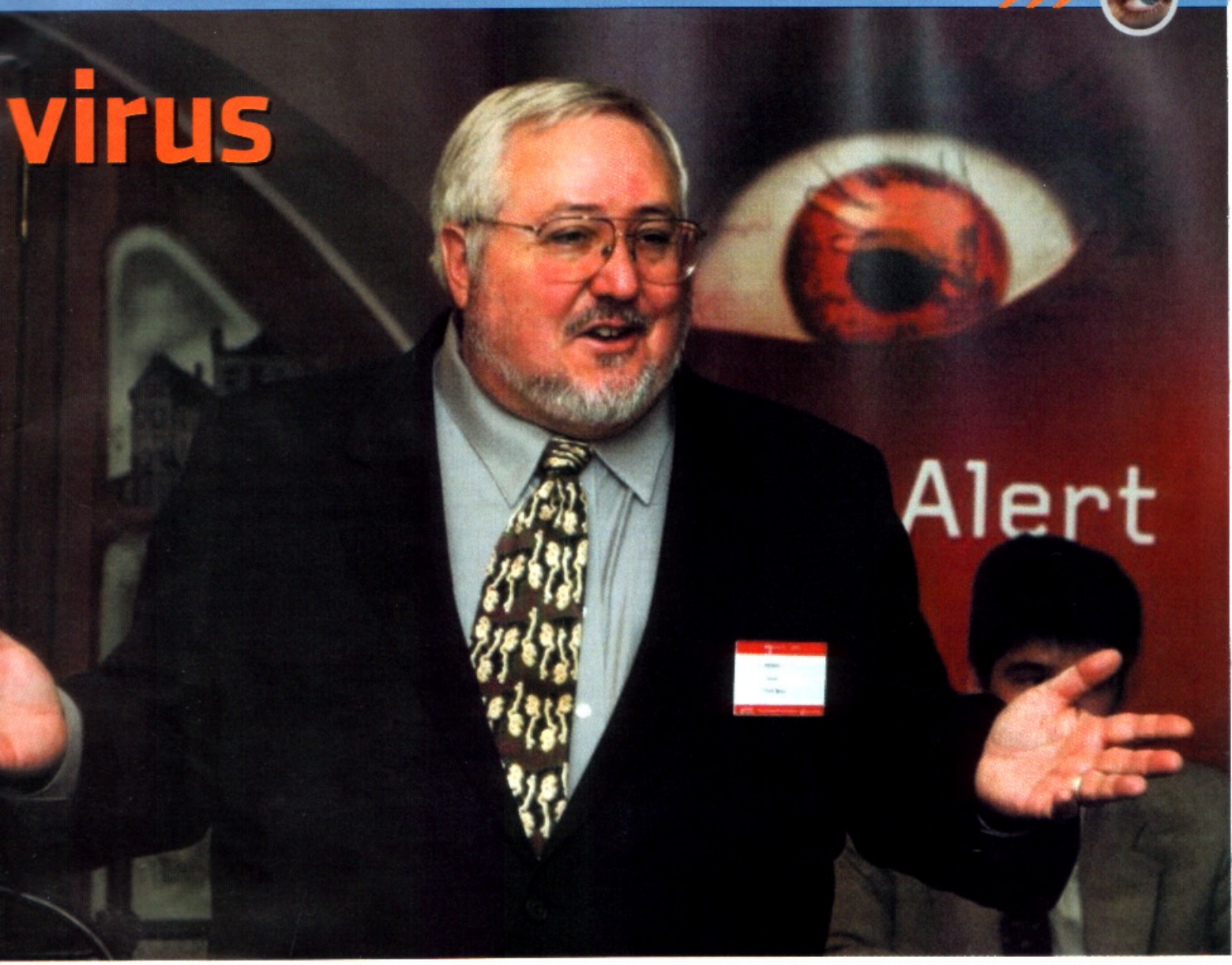
CHRONOLOGIE

1949 JOHN VON NEUMANN pose les bases de ce que seront les virus informatiques : des "automates cellulaires" capables de s'autorépliquer.

1970 JOHN CONWAY, le mathématicien qui a beaucoup contribué à la théorie du jeu, invente le "jeu de la vie" un automate cellulaire qui fonctionne à la manière d'un virus.

1971 LE VER CREEPER est le premier programme capable de se répande sur un réseau. Il affichait notamment *"Attrape-moi si tu peux !"*

1975 LE ROMANCIER DE SF JOHN BRUNNER écrit *Sur l'onde de Choc*. Dans son ouvrage, il évoque des programmes capables de passer d'un ordinateur à un autre sans se faire repérer.



"Je ne crois pas aux virus informatiques, ce sont des légendes urbaines, vous savez, comme ces crocodiles que l'on retrouve dans les égouts de New-York". Pendant ce temps, John McAfee, qui tenait à l'époque un BBS *(voir page 13)* qui faisait office de site de rencontre, se passionne pour le virus Brain et se dit : *"Tiens tiens, je vais peut être pouvoir faire de l'argent avec mon BBS !"*. Il engage un gamin de 19 ans pour s'en occuper, et Dave Chambers, un programmeur, pour développer la première version de McAfee Virus Scan. Très bon communicant, John McAfee s'introduit à la télé, dans les journaux et améliore son logiciel pour qu'il traite la petite centaine de ces premiers virus DOS comme Patagonia, Hamburger… Un peu jaloux de McAfee, Peter Norton se dit qu'il lui faut aussi un antivirus : il débauche Dave Chambers de chez McAfee pour qu'il écrive la première version de Norton Antivirus ! Je trouve ça génial : un seul gars a programmé les deux premiers antivirus de l'histoire ! Voici en tout cas comment l'industrie des antivirus a commencé, en réaction à ce seul virus Brain. Tous ces virus originels comme Elk Cloner, Brain voire Stoned, qui fit grand bruit aussi (il affi-

1982 ELK CLONER, le premier virus conçu pour agir sur les ordinateurs personnels, voit le jour.

1983 LE PROFESSEUR FRED COHEN, encore étudiant à l'unversité de Californie du Sud à l'époque, parle pour la première fois de "virus informatiques".

1986 DEUX FRÈRES PAKISTANAIS, Basit et Amjad Farooq Alvid, diffusent Brain, le premier virus écrit pour la plateforme PC d'IBM, ce qui lança le marché de l'antivirus.

1988 ROBERT MORRIS, étudiant en sciences informatiques, lâche un vers autoréplicant sur l'Internet. Les dégâts sont catastrophiques dans toutes les universités américaines.

chait une feuille de marijuana et annonçait que votre ordinateur était "stone") avaient un point commun : ils se répandaient par le lecteur de disquettes. On les appelait les virus de secteur de boot car ils s'installaient tous dans la zone d'amorçage dont disposait toutes les disquettes. Quand j'étais jeune technicien chez Symantec, je m'amusais d'ailleurs à modifier ce fameux secteur pour faire croire à mes amis qu'ils avaient des virus…

SVM : Quand sont arrivés les premiers virus destructeurs ?

D. P. : Au début des années 1990, un autre type de virus débarque : les virus de fichiers, qui se greffaient à des fichiers exécutables (.com, .exe, .bin, etc.). Il y en a rapidement eu bien plus que de virus de boot, mais ils se répandaient très peu, car à l'époque, les gens échangeaient beaucoup de disquettes et utilisaient des programmes piratés, ce qui était un excellent moyen de répandre les virus de boot, mais moins favorable aux virus de fichiers. En 1991, le premier virus de fichier destructeur est découvert à l'université de Jérusalem : Jerusalem B, également appelé Vendredi 13. Il a été écrit par un étudiant de l'université, mais personne n'a jamais su qui il était. Cependant Jerusalem B a remis les virus sur le devant de la scène, et attiré de nombreux médias. Si vous aviez le malheur de lancer un programme sur votre ordinateur un vendredi 13, ce virus l'effaçait purement et simplement. Jerusalem eut tellement de succès que de nombreux créateurs de virus s'en inspirèrent pour fabriquer des clones qui s'activaient le samedi 12, le vendredi 14, ou encore tous les vendredis sauf le 13, etc. !

> *"AVANT MICHELANGELO, ON NOUS APPELAIT 90 FOIS PAR JOUR ; APRÈS, C'ÉTAIT 7 000 FOIS*

En 1991, quelqu'un récupéra une copie de Stoned – que nous avons déjà évoqué – et la modifia pour en faire un autre virus destructeur qui se déclenchait pile une semaine avant un vendredi 13 – pour tromper ceux qui n'utilisaient pas d'antivirus – et effaçait les cent premiers secteurs de votre disque dur, ce qui rendait la machine inutilisable. Il fut prévu pour se déclencher le 6 mars 1992, date qui s'avère être l'anniversaire de Michel-Ange. D'où son nom, Michelangelo, même si le code ne contenait aucune référence à l'artiste… La machine médiatique s'emballa autour de ce virus susceptible de "détruire" tant de machines. John McAfee retourna a la télévision et annonca : *"Nous ne savons pas combien de gens vont être infectés par ce virus, cela pourrait être 5 000, cela pourrait être 5 millions"*.

Mine de rien, ce passage à la télé est un tournant dans l'histoire des virus informatiques. Je travaillais pour Norton à l'époque… Avant que McAfee ne passe à la télé, on nous appelait 90 fois par jour en moyenne. Après son passage, boum ! Nous passons à 7 000 appels par jour. Tout le monde dans l'entreprise, du chauffeur à la secrétaire en passant par les ingénieurs ont dû se mettre à répondre aux coups de fils de clients en panique. Nous étions obligés de travailler 24 heures sur 24 pour répondre à la demande. On dut même construire des douches dans les locaux pour se laver sur place ! Nous savions que tout cela allait s'arrêter après le 6 mars… La date fatidique arriva enfin et là, surprise : personne n'appella ! Rien, on pouvait entendre les oiseaux chanter dehors… En fait, il n'y eut pas de coups de fil ce 6 mars pour plusieurs raisons : soit parce que nos clients n'avaient jamais eu de virus, soit ils avaient eu le virus mais nous l'avions nettoyé, soit ils avaient bien été infectés par le virus sans se rendre compte que c'était Michelangelo. Ce même 6 mars, je reçois un fameux journaliste américain qui me supplie : *"David, montrez-nous un ordinateur qui a été détruit par ce virus !"* Il s'attend à voir un ordinateur littéralement démoli par Miche-

CARRIÈRE
Le virus de l'antivirus

À 53 ans, David Perry occupe le poste de directeur général pour l'éducation chez Trend Micro, un éditeur de solutions de sécurité basé à Tokyo. Il a débuté sa carrière dans la sécurité au support chez Peter Norton Computing (qui s'appelle désormais Symantec) et travailla ensuite chez McAfee Corporation.

1992 LA PANIQUE s'empare des médias à cause du virus Michelangelo.

1995 PREMIER VIRUS DE MACRO sur les documents Word.

1999 LE VER MELISSA, non destructeur, se propage à une vitesse incroyable par le biais d'Outlook, en contaminant tous les contacts d'un carnet d'adresses. Des variantes s'en prenaient aux fichiers systèmes.

2000 ILOVEYOU se répand sur le réseau comme une traînée de poudre. Il est considéré comme le virus le plus coûteux de l'histoire.

2003 BLASTER TERRORISE les nouveaux venus sous Windows XP. Il est capable de se loger dans la machine dès qu'elle se connecte à l'Internet.

langelo. Je lui montre un PC XT que j'avais infecté avec le virus, et je le relance. En fait, tout ce que faisait Michelangelo, c'était de bloquer l'ordinateur, qui n'affichait plus qu'un curseur DOS clignotant dans le coin supérieur gauche. *"C'est tout ? Vous vous êtes moqués de nous !"*, me dit-il. Il était fou ! Voilà en tout cas comment l'industrie de l'antivirus s'est développée, par l'emballement médiatique. Avant Michelangelo, Symantec n'avait que 10 000 utilisateurs dans le monde entier. Après, on était passé à 1,5 million.

Que se passe-t-il ensuite ? Un adolescent de Sofia, en Bulgarie, qui se fait appeler The Dark Avenger et aime coder des virus truffés de paroles d'Iron Maiden, crée The Dark Avenger Mutation Engine (DAME). C'est le premier programme capable de créer des virus "mutants". Ils sont particuliers car ils sont capables de s'auto-encrypter, ce qui les rend bien plus difficilement repérables pour les antivirus. Ils nous obligèrent à intégrer un logiciel d'émulation dans nos solutions, ce qui doubla la taille de nos programmes.

En 1995 le Pentium arrive, tout comme Windows 95, qui signe la mort des virus de boot : c'est en effet le premier OS à gérer le "mode protégé" d'Intel, qui empêche les virus de s'attaquer au secteur d'amorçage. Comme, par ailleurs les virus de fichiers sont toujours assez confidentiels à l'époque, on estime, chez Symantec, que l'ère des virus touche à sa fin et on envisage de délaisser le secteur. McAfee ne souhaite plus non plus être associé au monde des antivirus… Il rachète une compagnie appelée Network General, licencie tout le monde excepté quelques directeurs et renomme le tout Network Associates pour ne pas être assimilée à un éditeur d'antivirus, car il pensait que ce business était désormais invendable…

> *"DANS 10 ANS, IL FAUDRA BLOQUER UN MILLION DE NOUVELLES MENACES CHAQUE HEURE*

Et pourtant : 17 Juillet 1995, quelques mois avant la sortie de Windows 95, nous recevons une version bêta 2 de Windows 95 des mains mêmes de Microsoft (programme MSDN, *voir ci-contre*). Sur l'un des disques verts, que j'ai d'ailleurs encadré dans mon bureau, on trouve… le tout premier virus de macro au monde ! Il avait été écrit par un employé inconnu de chez Microsoft, et s'appelait Word Concept Macrovirus. Il n'était pas destructeur, mais insérait la phrase *"Je crois que cela prouve ce que je dis"* sur tous les documents auquel il accédait. Les virus de macro connurent par la suite un grand succès : plus faciles à écrire, car codés en Visual Basic, ils étaient aussi bien plus efficaces, car toutes les entreprises échangent des documents bureautiques de la suite Office. Au-delà du cercle restreint des pionniers de la micro-informatique, c'étaient les entreprises qui étaient désormais visées par les virus. Le 26 janvier 1999, je suis en vacances à DisneyWorld avec ma femme… Mon pager sonne : *"David, rappelle-nous en vitesse !"* Melissa, le premier virus diffusé par Internet, venait de débarquer. Melissa fut le dernier gros virus de macro, attaché à un mail et qui se propageait par Outlook.

SVM : Quelles sont les nouvelles menaces ?

D. P. : On le voit, l'évolution du malware est directement liée à l'évolution du matériel. En 1982, vous achetiez un micro capable de comprendre du langage Basic et de gérer une base de données. Pour le même prix aujourd'hui, vous avez une machine dotée d'une carte 3D surpuissante et connectée en permanence à Internet. Ces avancées technologiques offrent de nouvelles opportunités aux créateurs de virus. Aujourd'hui, les hackers amateurs qui ont créé les premiers virus sont toujours là. Cette année, il seront 12 000 à la Defcon, leur conférence annuelle… Mais les hackers ne sont plus le problème. Ils sont toujours là, mais sont éclipsés par des criminels organisés, des mafias qui aujourd'hui mènent la danse et font qu'on peut avoir chaque jour de 3 000 à 5 000 nouveaux virus, 25 000 à 30 000 nouvelles adresses Web à bloquer et des centaines de milliers de spams à contrer. D'après moi, dans dix ans, nous serons contraints de bloquer un million de nouvelles menaces chaque heure. Le plus grand danger aujourd'hui, c'est le Web : vous vous rendez sur une page, celle-ci a une iFrame (*voir ci-contre*) infectée par un virus dont l'objectif est d'implanter un "keylogger" (*voir article page 48*) dans votre système. Cela pour vous voler votre code de carte bancaire ou vos mots de passe… L'année dernière nous avons vu la première attaque Web massive : un FAI italien a eu 10 000 pages Web infectées par un malware, Mpack, que quelqu'un avait acheté à la mafia russe. Savez-vous que ces logiciels sont vendus avec un support technique ? Nous n'avons encore rien vu ! • **Propos recueillis par Éric Le Bourlout**

BBS
BBS, ou Bulletin Board System. C'est un peu l'ancêtre des forums : il s'agissait d'un serveur sur lequel les utilisateurs se connectaient pour échanger des messages ou des fichiers.

IFRAME
Une balise HTML qui permet d'intégrer un document dans un autre document. Elle est très utilisée pour insérer des vidéos ou des sons dans un site Internet… Et aussi par les pirates.

MSDN
Une offre que Microsoft propose aux développeurs Windows. En souscrivant à MSDN (Microsoft Developer Network), ils reçoivent tous les logiciels de Redmond en avant-première.

2005 UN ADOLESCENT CRÉE UN VER qui se propage sur Myspace. C'est sans doute le virus qui s'est le plus vite diffusé : en 20 heures, plus d'un million de profils Myspace se sont retrouvés contaminés. Le ver de Samy se contentait d'afficher *"Samy is my hero"* sur les pages des victimes.

2007 LE VER STORM contamine des millions d'ordinateurs à travers le monde, les transformant en zombies pour le botnet Storm.

2008 PREMIÈRES ATTAQUES MASSIVES SUR LE WEB. En mai, l'une d'entre-elles infecte un demi-million de pages Web.

Princes des hackers : le

De John T. Draper, qui piratait les centraux téléphoniques à la fin des années 70, au célébrissime Kevin Mitnick, *du groupe Cult of the Dead Cow à DVD Jon, le tombeur de la protection du DVD, portraits de hackers qui ont marqué leur époque.* • Par Bruno Mathé

CULT OF THE DEAD COW

Dealers pour les pirates en herbe

Ce célèbre groupe de hackers, créé en 1984, a développé une pléthore d'outils logiciels destinés à faciliter le piratage. Utilisé par des générations de "script kiddies" (néophytes sans compétences exploitant celles des autres), le plus connu est Back Orifice, qui utilise une faille de Windows pour permettre, de façon très simple, la prise de contrôle d'un ordinateur distant. Lancé en 1999 lors du Defcon (la convention annuelle des hackers à Las Vegas), Back Orifice a été suivi par une version 2000 – souvent acronymisée en BO2k – pour Windows 2000 et XP. Cult of the Dead Cow a récemment refait parler de lui avec Goolag Scanner, un outil permettant de trouver facilement les vulnérabilités des sites Web grâce à une utilisation judicieuse de Google. ■

LE SYSTÈME INFORMATIQUE DU "NEW YORK TIMES" EN TROPHÉE

Adrian Lamo

Le fait d'arme le plus connu de celui qui fut longtemps appelé "hacker sans domicile" pour son style de vie – il dormait chez des amis ou dans des squats – a consisté, en 2002, à s'introduire dans le système informatique du *New York Times*, récupérant au passage des informations confidentielles sur les employés, mais aussi les contacts des journalistes. Mais le palmarès d'Adrian Lamo est bien plus hétéroclite : Yahoo, Microsoft, AOL ou encore Mc Donald's comptent au nom de ses victimes. Invité sur NBC, il accède au réseau interne de la chaîne en 5 minutes. Adrian Lamo est aujourd'hui expert en sécurité. ■

Un jongleur dans le central téléphonique

Le hack mène à tout, la preuve : Kevin Poulsen (alias Dark Dante) est aujourd'hui journaliste et rédacteur en chef de Wired.com, la version en ligne du mensuel éponyme, spécialisé dans les nouvelles technologies. Le premier exploit du jeune Kevin, alors âgé de 17 ans,

Kevin Poulsen

consiste, en 1983, à s'introduire dans le réseau de l'Université de Californie (UCLA). Arrêté en 1989 pour avoir crocheté la serrure d'un central téléphonique Pacific Bell, il part en cavale. C'est durant celle-ci qu'il va commettre son hack le plus fameux : une radio promettant une Porsche au 102e auditeur qui appelle, Kevin Poulsen prend le contrôle des lignes téléphoniques de la station et gagne le véhicule. Lorsque l'émission de télé *Unsolved Mysteries* – une sorte de *Perdus de vue* local – évoque son cas, les numéros verts mis en place tombent mystérieusement en panne. Il sera finalement arrêté en avril 1991, poursuivi pour espionnage et très lourdement condamné : 51 mois de prison et 56 000 dollars de dédommagement à verser à Pacific Bell. ■

LE CASSE VIRTUEL DU SIÈCLE

Vladimir Levin

Le casse virtuel du siècle : c'est ce qu'a failli réussir le Russe Vladimir Levin en 1994. Il pirate alors le système informatique de la banque Citibank, accède à plusieurs comptes d'entreprises et fait virer 10,7 millions de dollars vers cinq comptes à l'étranger. Mais trois de ses complices sont arrêtés à Tel Aviv, San Francisco et Rotterdam lorsqu'ils tentent de retirer les fonds. Confondu, Levin est protégé par l'absence de traité d'extradition entre la Russie et les États-Unis. Cependant, une escale à Londres lui sera fatale : il est arrêté, en mars 1995, par Scotland Yard. Après une intense bataille juridique, il sera finalement jugé en février 1998 aux États-Unis et condamné à 3 ans de prison. Bien plus tard, en 2005, un hacker russe prétendra que Levin s'était, à l'époque du casse, contenté d'acheter pour 100 $ une porte dérobée du système de Citibank. ■

côté obscur du génie

EMBROUILLE DANS LE BROUILLAGE

DVD Jon

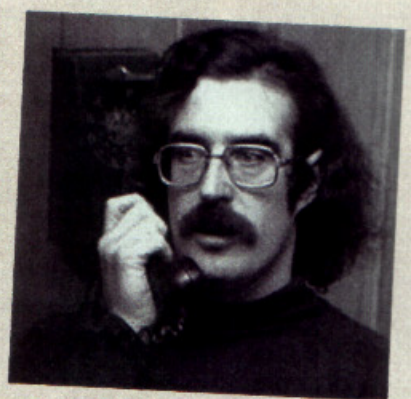
Son vrai nom, Jon Lech Johansen, est bien moins connu que son surnom, DVD Jon, qu'il tire de son premier fait d'arme : encore adolescent – il a alors 16 ans –, il fait partie du trio de programmeurs (les deux autres sont restés anonymes) du logiciel DeCSS, le premier à contourner le système de brouillage de contenu des DVD. DeCSS est publié, ainsi que son code source, en 1999 : c'est le début d'ennuis judiciaires qui dureront 4 ans, DVD Jon étant finalement acquitté. Mais pas la fin de ses exploits : en 2006 notamment, Johansen finit par casser le code de FairPlay, la technologie de gestion de droits numériques d'Apple verrouillant les chansons et vidéos de l'iTunes Music Store. La marque à la pomme a d'ailleurs les faveurs de DVD Jon : l'an dernier, il craque en partie la protection de l'iPhone une semaine après sa sortie, ouvrant la voie à d'autres hackers qui le déblo-queront totalement. DVD Jon travaille aujourd'hui pour DoubleTwist, un logiciel de synchronisation de contenus entre les PC et les baladeurs. ■

LE CONDOR FOND SUR LE PENTAGONE

Kevin Mitnick

Né le 6 Août 1963, Kevin Mitnick est sans doute le plus médiatique des hackers. Sa technique, c'est le "social engineering", où la faculté d'obtenir par la ruse des informations (mots de passe, numéros de téléphone, etc.) prime sur les compétences techniques. La légende veut que, dès ses 12 ans, il parvienne à tromper le système à cartes perforées utilisé par la société de bus de Los Angeles, voyageant ainsi gratuitement sur l'intégralité du réseau. En 1981, il pénètre – physiquement – dans un central téléphonique et s'amuse à faire quelques canulars aux abonnés. Mais se procure aussi de nombreux renseignements, lui permettant de détourner des lignes à son profit. Il sera arrêté et condamné à 3 mois en centre de redressement. En 1983, Kevin, qui se fait appeler Le Condor, parvient à s'introduire dans le système du Pentagone, via l'Arpanet (l'ancêtre d'Internet) : 6 mois de prison. La litanie des piratages suivis de condamnations se poursuit, notamment celui du système informatique de DEC (1 an de prison). En 1989, suite à une énième intrusion, le FBI vient l'arrêter à son domicile. Mais Mitnick s'enfuit. Il finira par être arrêté par le FBI après une traque de plus de 5 ans, grâce à l'aide d'un expert en sécurité informatique et ancien hacker lui même, Tsutomu Shimomura. Mitnick avait eu le tort de s'attaquer à lui le jour de Noël 1994. Il sera condamné à cinq ans de prison. Libéré en 2000, Kevin Mitnick dirige aujourd'hui sa propre société de sécurité informatique. ■

Il siphonne Bell avec un sifflet pour enfants



John T. Draper

Plus connu sous le surnom de Captain Crunch, qu'il doit aux boîtes de céréales Cap'n Crunch, vendues à la fin des années 60 avec un petit sifflet pour enfants. Lequel sifflet, découvrirent John T. Draper et son ami Joe Engressia (alias Joybubbles), émettait un son de fréquence 2 600 Hz, soit exactement celle utilisée par la compagnie téléphonique Bell pour indiquer qu'une ligne longue distance était libre et prête à recevoir un appel. L'ustensile servit au "phreaker" américain pour pirater Bell et passer gratuitement des appels longue distance. On lui prête ainsi un appel depuis une cabine téléphonique, traversant plusieurs dizaines de pays pour aboutir… à la cabine voisine. Captain Crunch fut condamné en 1971 à 5 ans de probation, inspira les fondateurs d'Apple, Steve Wozniak et Steve Jobs, qui débutèrent en vendant des boîtiers téléphoniques (blue box), travailla ensuite brièvement pour la compagnie à la pomme à la création d'une interface téléphonique pour l'Apple II, passa quelques mois en prison pour récidive, puis fonda sa société Cap'n Software. Il écrivit en 1979 le premier traitement de texte pour Apple puis pour IBM PC. Cet excentrique dirige actuellement en2go, une entreprise aux projets encore flous. ■

PHOTOS DR

Internet est-il vraiment solide?

Nous avons posé la question à Christophe Perrin, responsable du développement de marché sécurité chez Cisco France. *Un interlocuteur clé, quand on sait que toute connexion passe au moins une fois à travers un équipement de Cisco, mieux 80 % des informations circulant sur le Net le font grâce à ses technologies.* • **Propos recueillis par Delphine Sabattier**

interview

SVM : Le réseau a-t-il des faiblesses ?

Christophe Perrin : De quel Internet parlons-nous ? Pour les opérateurs, il y en a deux : celui sur lequel passe le trafic utilisateur et celui des "administrateurs" dédié à la configuration de leurs équipements. Ces réseaux sont faits de routeurs qui composent les "backbones" (les gros tuyaux de l'Internet, *ndlr*). C'est un peu la colonne vertébrale de l'Internet, et elle affiche une vraie solidité. Si un incident arrive du côté du trafic, un déni de service par exemple, l'opérateur peut continuer à utiliser ses équipements et remédier au problème. Le point le plus fragile du réseau Internet reste l'infrastructure DNS racine (les 13 serveurs à la base de la gestion des noms de domaine, *ndlr*) qui peut être la cible d'attaques.

SVM : Il y aurait donc deux réseaux identiques qui fonctionnent en parallèle ?

C. P. : Ces deux réseaux sont physiquement ou au moins virtuellement séparés. Le réseau administrateur a des besoins en débit de trafic très faibles, mais il est aussi largement déployé que celui utilisé pour transporter les informations des utilisateurs. L'opérateur garde toujours un peu de ressources processeur et de bande passante pour ce réseau de contrôle. Ainsi, même si la Toile est très encombrée, une partie du trafic peut être redirigée : les opérateurs détectent les anomalies et ils peuvent alors les isoler, voire les supprimer grâce à ce second réseau.

SVM : Comment le réseau de contrôle est-il sécurisé ?

C. P. : En premier lieu, on assure une redondance des équipements. Tout est doublé : les alimentations, les ventilations, les intelligences, les ressources processeur, les liens (pour le reroutage du trafic), les routeurs eux-mêmes... Ensuite, l'opérateur s'occupe de la traçabilité des manipulations, pour suivre en permanence les événements, les changements qui surviennent sur son réseau. Les processus de sécurité sont très poussés et respectent un code de "bonnes pratiques". Enfin, il y a un principe d'isolation qui doit s'appliquer : le réseau qui contrôle la configuration des équipements doit être totalement isolé et protégé de l'extérieur.

CHRISTOPHE PERRIN a une formation d'ingénieur télécom. Il s'est spécialisé dans la sécurisation des réseaux.

SVM : Cela suppose que tous les opérateurs respectent les règles de sécurité nécessaires...

C. P. : Tous ne déploient pas l'ensemble des bonnes pratiques, c'est certain. Mais l'un des atouts majeurs de l'Internet, c'est son concept collaboratif, distribué. Il existe ainsi des organisations dédiées à la gestion des alertes, les CERT (Computer Emergency Response Team), auxquelles tout le monde participe.

SVM : Peut-on dire qu'Internet est plus ou moins solide en fonction des zones géographiques ?

C. P. : En Asie, quelques ISP (opérateurs Internet, *ndlr*) ont connu des difficultés, mais c'est resté très isolé. Les incidents de coupure sont rares, localisés, et en cas de problème, il est toujours possible de passer d'un opérateur déficient à un autre, resté opérationnel (si l'entreprise a des connexions vers plusieurs opérateurs). On n'a jamais vu Internet tomber. Si cela arrive un jour, ce sera pour des raisons politiques, pas techniques. ●

PHOTO DR

Nouveau !

Découvrez aussi l'AntiVirus Firewall Pro pour protéger jusqu'à 10 PC et centraliser la sécurité de vos PC !

Edouard et Aurélie PADDEBOL-LAPOISSE
Emmanuelle et Lucie PADDEBOL ses propriétaires,

Monsieur Alexandre DERNIÉCRI son créateur,

Monsieur Mathieu ILÉSUPER son revendeur,

Monsieur Renaud PEURIENFER son réparateur,

Et tous ceux qui s'en sont servis,

ont la tristesse de vous faire part du décès accidentel de leur ordinateur

PC chéri

Né AA02/B563-698/852-04Z

survenu à son domicile, le 31 août 2006, à l'âge de 3 ans.

Dans l'attente de ses funérailles, sa tour repose dans le bureau des Paddebol,
666 rue de la Malchance à Crasseville.
Visites de 19h15 à 19h20.

CET AVIS TIENT LIEU DE FAIRE-PART
Ni fleurs, ni couronnes
59 951 CRASSEVILLE - 666 rue de la Malchance.

Pour éviter de perdre à jamais vos ordinateurs, il y a Securitoo Antivirus Firewall.

Trouvez enfin la paix de l'esprit grâce à l'**AntiVirus Firewall avec anti-spam et anti-spyware Securitoo.**
Lors de chaque connexion Internet, l'AntiVirus se met automatiquement à jour et récupère les dernières signatures de virus.
Vous bénéficiez ainsi d'un niveau de protection optimal pour vos PC. Mortel, non ?

Abonnez-vous au 0 890 71 20 11 ou sur www.securitoo.com

Securitoo AntiVirus Firewall

Pour seulement **5€**TTC / mois

Protection immédiate de vos PC
Plusieurs moteurs d'analyse virale
Blocage des tentatives d'intrusion
Alertes instantanées

www.securitoo.com

NordNet

Les pirates fondent sur les

***Les applications hébergées et les réseaux sociaux** ont le vent en poupe. Mais leur succès en cache un autre : celui des virus, vers et pages de phishing qui se nourrissent de leur popularité.*

Octobre 2005. Un petit génie de l'informatique de 19 ans, qui répond au pseudo de Samy, a la subite envie de devenir le plus populaire des utilisateurs de MySpace : il crée un programme d'une quarantaine de lignes, qu'il insère sur sa page MySpace. Un ver, plus précisément, qui fonctionne de la manière suivante : dès qu'un membre de Myspace visite son profil, ce virus ajoute automatiquement Samy à sa liste d'amis. Mieux, il se réplique automatiquement sur le profil de la victime qui à son tour contamine les amis qui viennent lui rendre visite, tout en plaçant le modeste message *"Samy is My Hero"* sur chaque page et en enrichissant à chaque contamination la liste de contacts de Samy. Voilà comment, en quelques jours, Samy est devenu le "héros" d'un bon million d'utilisateurs de MySpace… avant que le site ne tombe et que l'équipe ne corrige finalement la faille. *"Le programme de Samy était bien plus facile à réaliser qu'un cheval de Troie ou un virus traditionnel. Il n'a pas eu besoin de le compiler, il était facile à placer dans une page et Samy a pu ainsi se livrer à toutes les expérimentations qu'il a souhaitées"*, précisait Don Hubbard, vice-président de la recherche en sécurité chez Websence lors d'une conférence.

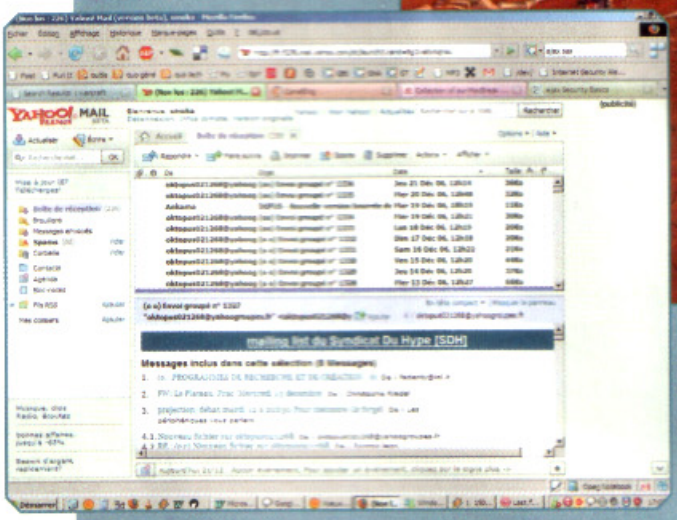
1. AJAX
C'est la technique de programmation du Web 2.0, qui permet d'avoir des pages dynamiques. Revers de la médaille : Ajax peut être également utilisé par des pirates pour pourrir discrètement des sites.

2. XSS
"Cross Site Scripting", est une faille de sécurité dans les sites Web qui permet d'y placer du code sans y être autorisé. Une plaie pour les services Web 2.0, sur lesquels l'utilisateur est souvent libre de placer ce qu'il veut.

3. PHISHING
Ou "hameçonnage". Le phishing consiste à se faire passer pour quelqu'un d'autre afin d'obtenir des informations personnelles. Très utilisé pour le vol d'informations bancaires, il a fait une entrée fracassante dans les services Web 2.0, riches en données utilisateurs.

Un immense vivier à hameçonner

Les experts en sécurité prennent souvent l'exemple de Samy pour évoquer les menaces pour la sécurité informatique de ce Web 2.0 et du langage de programmation Ajax, grâce auxquels tout le monde publie et communique dans des réseaux étroitement tissés. Des centaines de millions de pages Web liées les unes aux autres, très faciles à modifier pour y placer du code, sont ainsi mises à jour en permanence sur Internet. Et parmi tous ces services, MySpace est sans conteste le plus violemment attaqué par les pirates. Et pas seulement par des attaques XSS *(voir lexique)* comme celle de Samy. Début décembre, ce site a aussi été la victime d'un hameçonnage (phishing, *voir aussi page 22*) particulièrement pervers : une vidéo Quicktime incluse dans certains profils contenait un Javascript renvoyant les victimes vers une fausse page d'identification. Les pirates ont ainsi pu récupérer des centaines d'identifiants de connexion. Le phénomène phishing a réellement décollé en 2006 et n'a fait que se développer depuis. Les messages de ce type interceptés par un spécialiste de la sécurité comme Symantec se comptent en milliards chaque année. La faute au Web 2.0 ? Pas seulement, les tentatives de phishing passent avant tout par le canal du courrier électronique. Mais ces nouveaux services en ligne, sur lesquels les internautes entreposent beaucoup d'informations personnelles, attirent incontestablement les pirates et vont de fait amplifier le phénomène.



WEBMAILS Yahoo Mail a été la victime éphémère d'un ver Javascript, qui passait de boîte mail en boîte mail lorsque l'utilisateur affichait le message contaminé. Yahoo a heureusement corrigé la faille sans tarder.

FLUX RSS Ils pourraient bien devenir des vecteurs de virus : il est en effet tout à fait possible d'y cacher du code… capable de cibler différents lecteurs de flux ou un lecteur en ligne chez qui le pirate a trouvé une faille.

communautés

JEUX EN LIGNE L'économie virtuelle générée par les jeux en ligne attire les pirates. Le jeu de rôle Lineage,et maintenant World Of Warcraft (*ci-contre*), ont été les victimes de pirates désireux de récupérer les identifiants et mots de passe de joueurs.

LES PRÉCAUTIONS À PRENDRE

Pour éviter le vol d'informations personnelles, nous ne saurions trop vous conseiller de vous munir d'un navigateur récent, comme IE7 ou Firefox 3, qui comprennent tous deux des protections antiphishing. Votre antivirus et des logiciels dédiés comme SiteAdvisor ou Norton Confidential apportent une couche de protection supplémentaire. En règle générale, évitez de laisser trop d'informations personnelles sur les sites (ou inventez-les) et utilisez des identifiants et mots de passe différents sur ceux que vous fréquentez. Méfiez-vous aussi de certains services de réseaux sociaux – comme Ringo, très connu des utilisateurs de Windows Live – qui sont de véritables usines à spam vous demandant même votre mot de passe Passeport, histoire de se propager dans la boîte aux lettres de tous vos contacts...

RÉSEAUX SOCIAUX MySpace, le plus populaire des réseaux sociaux, est aussi le plus attaqué. Tentatives de phishing, failles XSS... MySpace a été la victime du premier ver "Web 2.0". Bénin, il a été programmé par un jeune de 19 ans.

Certains utilisateurs du webmail de Yahoo, écrit tout en Ajax, ont aussi été victimes de ces nouvelles formes de piratage : profitant d'une faille du service, des hackers ont lancé un ver en Javascript qui, par le biais d'un simple courrier HTML, contaminait la boîte de la victime, récupérait ses contacts, se dupliquait dans sa boîte et envoyait l'ensemble des adresses vers un site tiers. Yahoo a vite corrigé la faille, qui n'a en définitive fait que très peu de dégâts. Il n'empêche, ces attaques, contre lesquelles même votre vaillant antivirus ne peut pas grand-chose, inquiètent. Désormais, des virus pourraient vous causer du souci sans même toucher à votre PC.

Qui veut jouer avec les pirates ?

Finis les vieux virus de macro dans Word, dépassé le quasi-monopole du duo Internet Explorer-Outlook qui recensait, il y a peu encore, la plupart des menaces. Toutes les applications qui ont un contact avec l'Internet peuvent désormais être concernées par ces virus : on ne compte plus, par exemple, les malwares qui se répandent par messages Windows Live Messenger (ex-MSN). Facebook en a lui aussi été la victime début 2008, par le biais d'une application tierce qui pointait vers un virus. Même les jeux vidéo en ligne ne sont plus exempts de menaces : début juin, Blizzard, l'éditeur de World of Warcraft a prévenu les joueurs du plus populaires des jeux de rôles en ligne : une faille dans le plug-in Flash peut permettre à des pirates d'installer un virus sur leur machine et de récupérer leurs identifiants, le tout pour voler leur précieux compte. Alors un conseil : quoi que vous fassiez sur le Web, attention à vos données personnelles ! • **E.L.B.**

MESSAGERIES Un cheval de Troie est véhiculé par Skype : certains utilisateurs ont reçu un message d'un ami leur demandant de télécharger un fichier, en fait un virus dont l'objectif est de voler des informations personnelles. Windows Live Messenger est aussi victime de ce genre d'attaque.

Le Web 2.0, un village

***Sur Internet, la mode est au "contenu généré par les utilisateurs"** et aux réseaux sociaux. Des sites qui gardent une foule d'informations personnelles, et qui pourraient bien, à terme, menacer votre vie privée…*

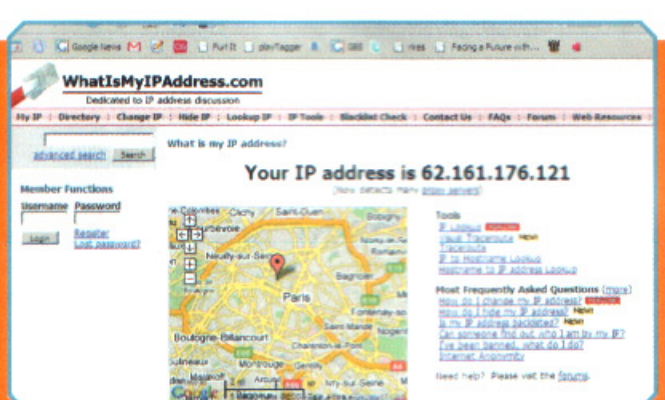
Mot de passe
3Xb28y7z
Adresse IP
62.161.176.121

Attention aux traces que vous laissez sur le Net ! De nombreux services que vous utilisez au quotidien enregistrent, à votre insu ou non, une somme considérable d'informations personnelles. On sait depuis longtemps que des journaux de chats, les forums et autres points de rencontre sur Internet pouvaient en dire beaucoup sur vous et votre entourage… Mais avec l'émergence du Web participatif, la tendance ne fait que s'accentuer. Des dizaines de sites parmi les plus populaires sur Internet à ce jour ne sont d'ailleurs que cela : des réceptacles à infos personnelles, aux bases de données remplies de messages, photos, vidéos entreposés par des millions d'internautes, qui leur confient une part grandissante de leurs données personnelles. TypePad, MySpace, Facebook, Flickr… Autant d'entreprises pour qui vous représentez des dollars sonnants et trébuchants et sur lesquelles vous pouvez compter pour analyser de près vos préférences, hobbies, films ou livres préférés. Leur trésor, c'est ce que vous leur confiez.

Votre vie privée est-elle en danger, à l'heure du Web 2.0 ? Nombreux sont les experts en sécurité informatique à le penser. D'abord parce qu'on ne contrôle pas tout ce que l'on poste sur Internet, à la vue de tous. La publication d'un simple billet de blog peut, par exemple, avoir des conséquences graves. Aux États-Unis et au Royaume-Uni, plusieurs blogueurs ont été licenciés pour avoir tenu sur leur site des propos contre leur entreprise ou leur patron, à l'image de "Petite Anglaise", une Britannique expatriée à Paris, virée par un chef qui a découvert sur son blog l'opinion qu'elle avait de lui, sans qu'il y soit jamais nommé, pourtant. Et que penser de Loïc, internaute peu malin qui avait posté sur YouTube une vidéo où on le voyait rouler à plus de 100 km/h en ville… Une "performance" tombée sous les yeux d'un policier qui a croisé les informations glanées

MAIS QUE RÉVÈLE VOTRE IP ?

Cette suite de quatre nombres que vous octroie votre FAI est capable d'en dire beaucoup sur vous. Pour en avoir la preuve, rendez-vous donc sur le site http://whatismyipaddress.com. Vous allez y voir apparaître votre IP avec, à côté, un petit plan Google situant votre position géographique. Cette localisation grâce à l'IP, qui peut-être plus ou moins précise, est souvent utilisée par des publicitaires peu scrupuleux, qui vous proposent des fausses annonces de rencontres près de chez vous via des bannières suggestives.
De même, à chaque fois que vous vous rendez sur un site, votre IP est loguée pour plusieurs raisons : vous proposer des pubs ciblées ou tout simplement garnir les statistiques du site. Le webmestre peut de cette façon vous identifier, savoir combien de pages vous avez consulté, examiner votre parcours, identifier les rubriques du site qui vous ont intéressé. Idem sur les blogs, qui possèdent pour beaucoup un outil de statistiques très performant qui intègre un outil de localisation. Méfiance, donc, si vous passez votre temps à espionner le blog d'un de vos proches : S'il est un peu soupçonneux, il lui suffira de quelques secondes pour deviner qui se cache derrière ce visiteur mystère.



où tout se sait

dans la vidéo (prénom, modèle de la voiture, etc.) avec le fichier des automobilistes. Résultat : procédure pour mise en danger de la vie d'autrui.

Méfiez-vous aussi de vos proches

Sans même poster des vidéos compromettantes, les sites communautaires peuvent s'avérer d'excellents mouchards si vous les utilisez intensément sans faire attention à vos données. Avec eux, même plus besoin de votre IP pour vous pister. Il est facile par exemple d'en apprendre beaucoup sur vous en surfant sur les pages de vos amis sur lesquelles vous avez laissé des commentaires, ou faire une recherche sur votre pseudo pour trouver d'autres services auxquels vous êtes inscrit *(voir nos conseils en colonne de droite)*. Pire, les réseaux sociaux, qui se sont tous répandus à la manière des virus – c'est-à-dire en contaminant vos amis, puis les amis de vos amis en les incitant à s'inscrire à leur tour – se dotent depuis quelques mois de nouvelles fonctions pour doper leur audience. Twitter, Last.fm, Facebook et d'autres proposent de fouiller le carnet d'adresses Gmail d'un de leurs membres à la recherche de contacts eux-mêmes abonnés à leur service, afin de les ajouter ensuite à ses amis. Si vous utilisez votre adresse mail habituelle, vous risquez donc d'être lu par des connaissances, sans même que vous le sachiez.

Cette fonction illustre bien ce qu'est en train de devenir le Web : un tissu de services entremêlés, capables de partager des données entre eux par le biais d'interfaces conçues par leurs développeurs. Une Toile sur laquelle on livre de plus en plus d'infos, et chaque jour plus transparente. Dangereux ? Sans conteste. Gunter Ollmann, directeur de la stratégie de sécurité chez IBM, l'évoque dans un article publié récemment : pour des hackers mal intentionnés, les réseaux sociaux sont pain bénit, aussi bien pour voler l'identité d'un individu que pour attaquer une entreprise. Ollmann explique notamment comment un pirate pourrait se servir des données du réseau social professionnel Linked In afin de dénicher des informations très précises sur les collaborateurs d'une même entreprise, de leur famille, de leurs loisirs, avant de déclencher une attaque hyperciblée : *"En quelques minutes, on pourrait attaquer de multiples personnes d'une même entreprise… Et envoyer des e-mails très personnels, censés venir d'un ami proche, avec des 'photos' de la dernière fête au lac."* La victime reconnaîtra l'adresse d'un ami, les photos de la fête (en fait, elles étaient sur Flickr), mais ne se doutera pas que du code malicieux lui a été envoyé en même temps, installant un logiciel malveillant dans sa machine…

Une illustration de ce qui peut arriver dans ce monde nouveau du Web 2.0, si on ne fait pas attention à ce qu'on y stocke. Alors gare ! • **E.L.B.**

LES RÈGLES DE BASE

- **ÉVITEZ AU MAXIMUM DE DONNER VOTRE VÉRITABLE NOM** sur Internet, surtout à des services comme les réseaux sociaux. De même, les formulaires des sites vous invitent souvent à leur donner de nombreuses informations personnelles pour garnir leurs fichiers de précieuses infos. Attention également à décocher toutes les boîtes de dialogue des sites qui proposent de fournir vos informations personnelles "à leurs partenaires".
- **RESTEZ TOUJOURS MAÎTRE DE VOTRE IDENTITÉ.** Il peut être utile de conserver son véritable nom sur un réseau social professionnel tel que Linked In, mais si vous utilisez plusieurs pseudos, attention à ne pas les mélanger sur un même site. Par exemple en ajoutant à votre profil un service extérieur auquel vous êtes abonné sous un autre nom.
- **SI VOUS CESSEZ D'UTILISER UN SERVICE,** prenez la peine de vous désabonner (ce qui est parfois difficile à faire), afin de supprimer tout ce que vous avez partagé. Sinon, on pourra toujours retrouver vos infos par le biais des moteurs de recherche.

Phishing : gare aux

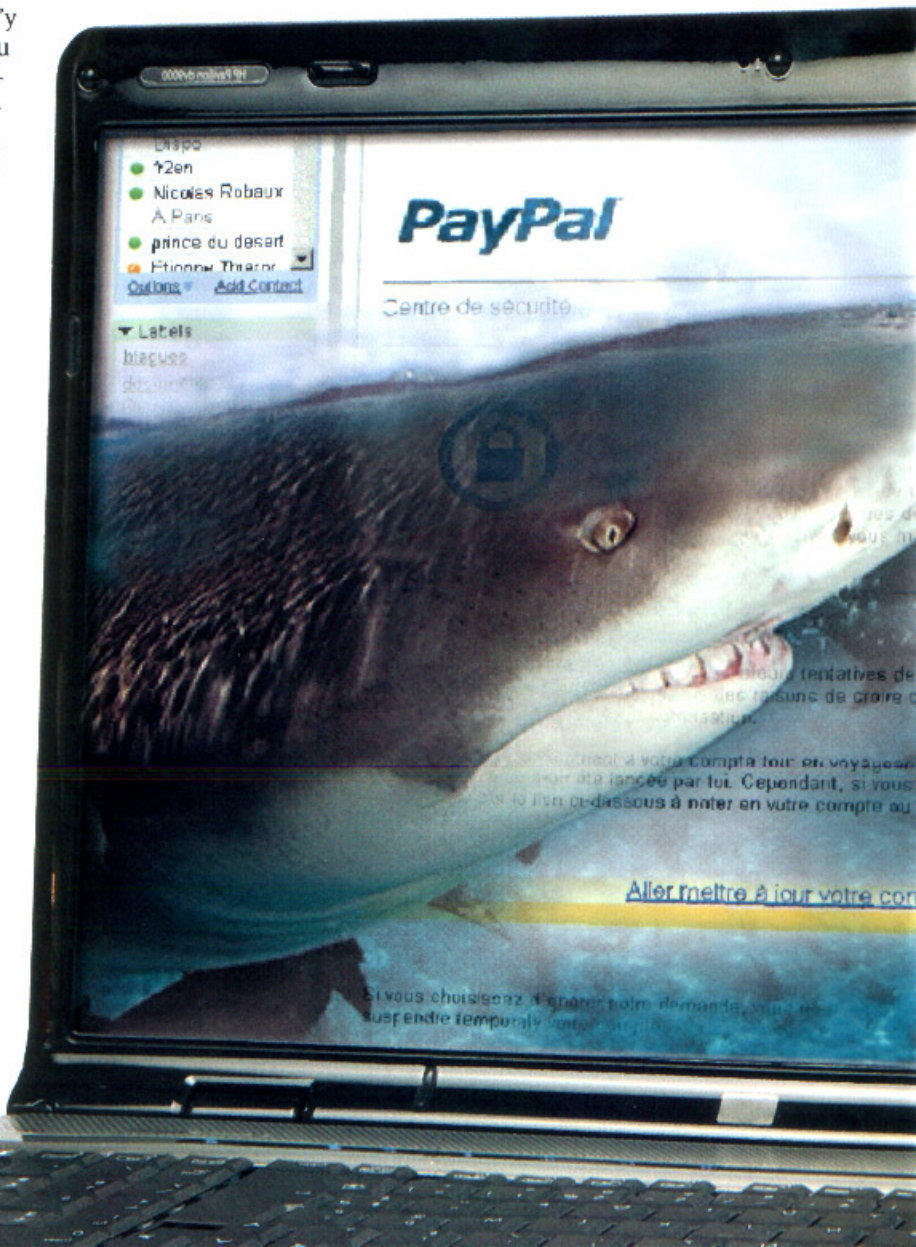
C'est une des plaies de l'Internet. *Et malheureusement, le phishing n'est pas près de disparaître. Il aurait au contraire tendance à prendre des formes bien plus malignes qu'auparavant.*

Rappelons d'abord en quelques mots en quoi consiste "l'hameçonnage" (phishing en anglais) : vous recevez un mail provenant apparemment de votre banque. Qui, étonnamment, vous demande de confirmer vos détails bancaires, autrement dit d'entrer votre identifiant et votre mot de passe. Il est vrai qu'il y a de quoi se tromper, car le mail reprend le logo de la banque, la même typographie… Tout juste y remarque-t-on parfois une faute d'orthographe parci par-là. Mais gare ! Le mail a été écrit par un criminel qui cherche à voler votre identité bancaire grâce à cette technique d'ingénierie sociale (*voir page 28*) de masse. Associé au message, un site qui imite à la perfection celui de votre banque a été mis en place par le pirate. Si vous avez le malheur d'y entrer vos identifiants, vous pouvez dire adieu à vos économies… Et ce ne sont plus seulement les banques qui sont concernées : désormais, même vos identifiants Youtube, Gmail, Fnac, iTunes… intéressent les pirates à la recherche de mots de passe.

Fausses pages dans des sites officiels

La technique est d'autant plus efficace qu'elle est très simple à mettre en œuvre. Pas besoin d'être un hacker confirmé pour se lancer dans une attaque de phishing. Il existe d'ailleurs un "kit du phisheur en herbe", vendu sous le manteau sur Internet, qui ne cesse de se perfectionner de mois en mois. Son nom : Rock Phish. Il permet de créer en quelques minutes une campagne complète de phishing en copiant des dizaines de sites différents, sans connaissances techniques particulières. Son seul "défaut" ? Toutes les fausses pages sont hébergées sur un seul et même domaine : ci celui-ci vient à être découvert, plus aucune des autres fausses pages ne fonctionnera.

Mais, de plus en plus malins, les pirates adeptes du phishing utilisent de nouvelles techniques pour tromper les internautes. D'abord, ils se servent des réseaux de machines zombies d'internautes lambda (botnets, *voir page 48*) pour héberger leurs fausses pages Web. Qui sont du coup plus difficile à débusquer… Et si ces ordinateurs sont un jour "blacklistés", il suffit d'en prendre d'autres, ce qui permet de faire durer une campagne de phishing bien plus longtemps. Plus grave encore, on constate aussi désormais que certains sites tout à fait officiels abritent, sans le savoir, des pages de phishing insérées par des pirates, parce que le site était vulnérable à des attaques par "injection SQL". Le consultant en sécurité Dancho Danchev dévoilait récemment sur son blog (**http://ddanchev.blogspot.com/2008/06/uks-crime-reduction-portal-hosting.html**)que la poste italienne avait par exemple été victime d'un hameçonnage hébergé… sur un site officiel britannique ! Là encore, il devient plus compliqué, du coup, de le fermer. Autre technique en plein essor : le "spear phishing", qu'on pourrait traduire par "hameçonnage de pointe".



requins de l'e-mail !

L'agression, contrairement aux attaques traditionnelles est ici ultraciblée afin de paraître particulièrement crédible à tous les visiteurs d'un site spécialisé, ou à tous les employés d'une entreprise... Par exemple, un pirate peut se faire passer pour votre responsable réseau et vous demander votre identifiant et mot de passe.

Difficile de remonter la piste

Lutter contre le phishing est encore plus complexe que de se battre contre les codes malicieux. Les versions récentes des navigateurs Web (Firefox 2 et 3, IE 7 et 8) contiennent pourtant un dispositif antiphishing : basé sur une liste de sites blacklistés, il est efficace... si la menace a déjà été repérée quelque part. Les suites de sécurité fournies par les éditeurs d'antivirus disposent également de procédures plus avancées pour tenter de dénicher un message frauduleux (*voir page 48*) mais ne peuvent, elles non plus, garantir une protection à 100 %. Il faut donc avant tout rester vigilant. Établissements bancaires et sites marchands ne demandent de toute façon jamais un identifiant et un mot de passe par le biais d'un mail (*voir nos conseils ci-contre*).

Quant aux responsables de ces attaques, ils restent la plupart du temps impunis. Ou presque. Début mai, la police met la main sur quatre jeunes internautes soupçonnés d'avoir participé à une arnaque par phishing. Chez eux, on retrouve du matériel high-tech et des bordereaux Chronopost mentionnant un destinataire en Tunisie. En fait, ils ont été "recrutés" comme mules par un pirate tunisien adepte du phishing, qui s'est servi d'eux pour son arnaque : il obtenait d'abord l'accès à des comptes Paypal en hameçonnant des internautes, puis virait une somme variable du compte Paypal des victimes vers celui de ses complices. Ces derniers achetaient ensuite du matériel, toujours par Paypal, et renvoyaient vers la Tunisie la moitié de leurs "cadeaux". Une vingtaine d'utilisateurs de Paypal ont été victimes de la bande. Si les quatre jeunes ont bien été interpellés, l'arnaqueur, dont l'identité a été révélée, court toujours. Il a d'ailleurs conservé un site spécialisé dans les téléchargements de contenus piratés qui fait le plein de visiteurs... Et ne semble pas s'inquiéter outre mesure de toute cette affaire. À une toute autre échelle, trente-huit pirates roumains et américains viennent d'être inculpés pour avoir participé à un vaste réseau de phishing bien plus complexe. Les pirates roumains récupéraient des codes de cartes bancaires par phishing, qu'ils transmettaient par chat à des complices aux États-Unis : d'abord à des fabricants de fausses cartes bancaires, qui fabriquaient des exemplaires falsifiés puis les transmettaient à d'autres individus ; ces derniers les utilisaient pour effectuer des retraits. Enfin, tous se partageaient le magot. Face à de telles organisations criminelles, on comprend mieux pourquoi il est difficile d'en finir avec le phishing ! **E.L.B.**

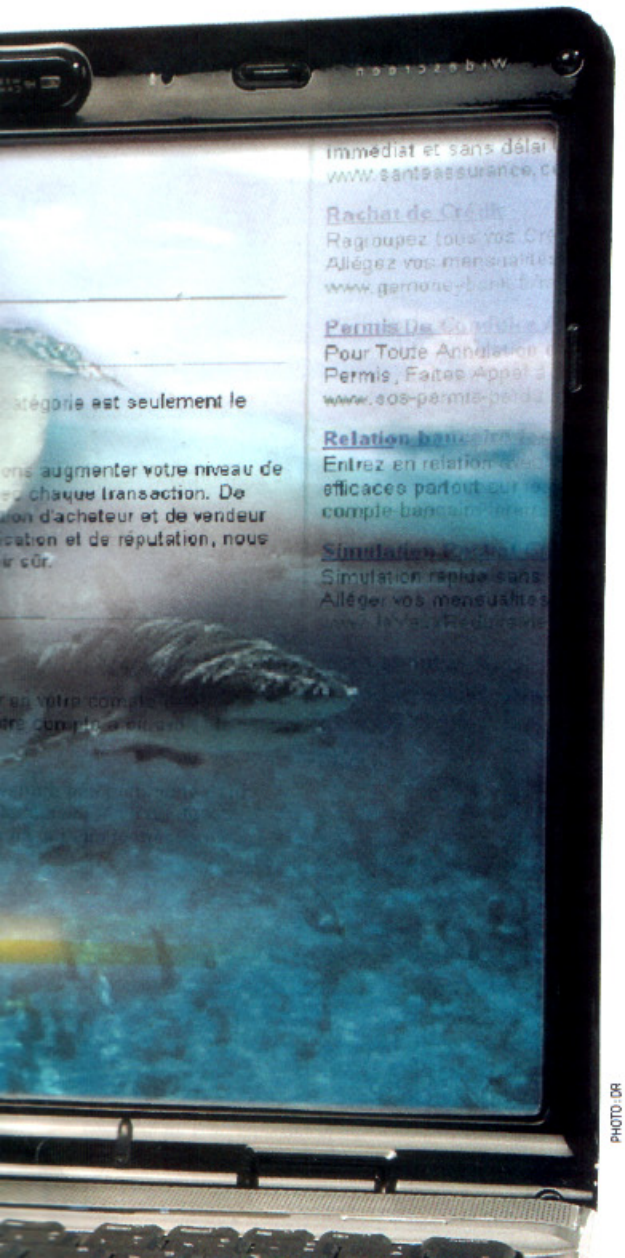


PHOTO : DR

QUATRE CONSEILS POUR ÉVITER DE SE FAIRE PIÉGER

1. Ne répondez à aucun mail provenant de votre banque, de Paypal ou d'un site marchand vous demandant de redonner vos identifiant et mot de passe.
2. Si un mail vous paraît louche, ne faites pas confiance à l'adresse e-mail, facilement modifiable. En revanche, les URL des sites de phishing ressemblent fort à l'adresse classique, mais sont forcément différentes.
3. Si vous avez été victime d'un phishing et que vous vous en rendez compte immédiatement, changez en vitesse votre mot de passe pour empêcher les pirates de pénétrer votre compte.
4. Dans tous les cas, si vous vous êtes fait piéger, contactez immédiatement votre établissement bancaire pour le prévenir de votre situation.

Scam : les virtuoses de

***Pour soutirer de l'argent, les scammeurs font miroiter monts et merveilles** à leurs victimes : un pourcentage sur une grosse somme d'argent à transférer, un gain à la loterie, une romance, une bonne action… A l'arrivée, certaines se font dépouiller de plusieurs dizaines de milliers d'euros.*

Le neveu d'un gouverneur de banque centrale emprisonné ou la fille d'un haut responsable condamné à l'exil ; une importante somme d'argent à faire sortir du pays et un gros pourcentage pour celui qui acceptera de faire transiter le pactole sur un compte en Europe. Voilà les ingrédients du spam nigérian, aussi appelé "scam". Qui n'a pas reçu une de ces propositions alléchantes et fait le calcul dans sa tête : 20 % de 30 millions de dollars = 6 millions sans rien faire, juste en servant d'intermédiaire. C'est tentant. Sauf qu'à l'arrivée bien sûr, il y a une grosse arnaque. En décembre dernier, le tribunal correctionnel de Strasbourg a condamné trois scammeurs camerounais pour escroquerie en bande organisée. Ils se faisaient passer pour la veuve de l'ex-président du Niger, assassiné en 1999. Cette dernière recherchait soi-disant une personne de confiance pour transférer 28 millions de dollars en France. L'intermédiaire devait toucher 20 % de la somme, à condition bien sûr d'avancer certains frais. Pour commencer, un faux notaire demandait 3 000 euros pour la rédaction de documents officiels. Il fallait ensuite payer le gardiennage de l'argent, les taxes de douanes, de multiples pots de vin... Les escrocs ont même fait le coup du "wash-wash", essayant de faire croire que les billets noircis pour des raisons de sécurité, bien sûr faux, devaient être lavés afin de retrouver leur aspect d'origine. Un grand classique du scam.

Au bout du compte, l'une de leurs victimes a versé plus de 35 000 euros aux trois hommes, qui auraient récupéré au moins 50 000 euros en tout grâce à cette arnaque. L'histoire est exemplaire et malheureusement assez banale. Quelques mois plus tôt, une affaire similaire était jugée à La Roche-sur-Yon. Les six prévenus avaient récolté près de 200 000 euros grâce à une campagne de mails identique. Parmi les victimes, deux consultants hollandais qui espéraient faire une bonne affaire et qui ont déboursé jusqu'à 150 000 euros.

La convoitise endort la méfiance

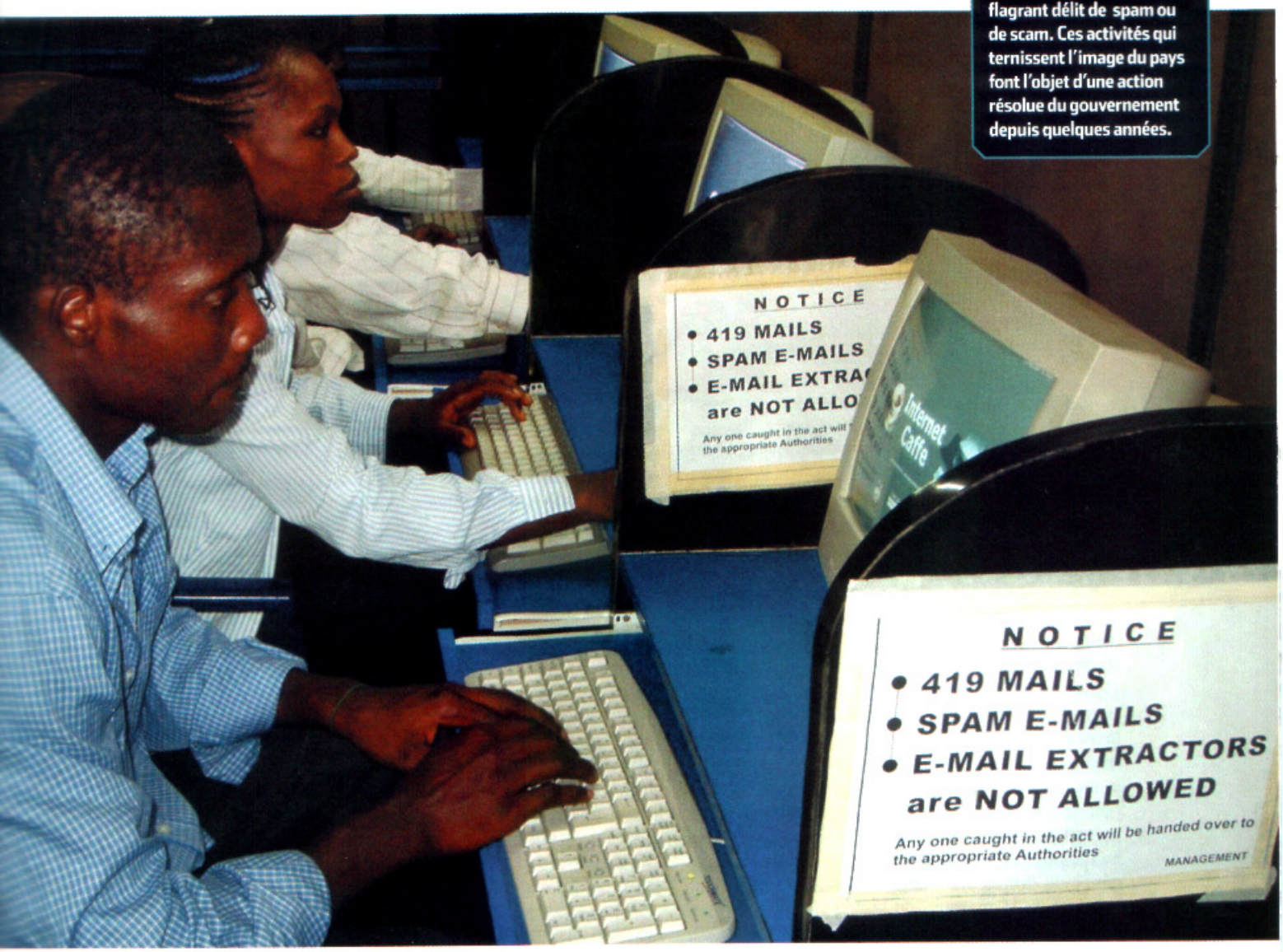
Contrairement à ce qu'on pourrait penser en lisant ces mails parfois mal orthographiés, le scam rapporte. Les sommes détournées peuvent être très importantes. Début 2006, les autorités néerlandaises ont arrêté douze individus à Amsterdam, soupçonnés d'avoir soutiré plus de 2 millions d'euros. La plupart des internautes ne tombent pas dans le panneau, mais il suffit que 1 % des personnes contactées se laissent convaincre pour que l'affaire soit rentable. Pour tromper la méfiance des internautes, les scammeurs multiplient les variantes. Parmi les grands classiques, le transfert de fonds bien sûr, mais aussi le gros lot à la loterie. Le mail annonce à la victime potentielle qu'elle a été tirée au sort et qu'elle a gagné une coquette somme d'argent. La procédure pour récupérer le pactole nécessite bien entendu le paiement de quelques menus frais de gestion. La fausse offre d'emploi est moins courante, mais plus convaincante. Les scammeurs prétendent être une entreprise à la recherche de collaborateurs dans un pays africain. La rémunération est bien sûr attractive, les à-côtés – voiture et logement de fonction – appréciables. L'offre, évidemment, est fictive, mais les victimes sont tenues de débourser quelques deniers pour les permis de travail ou le voyage. *"Les auteurs de ce type d'escroquerie jouent sur une corde sensible, l'appât du gain ou la libido"*, explique le commissaire Yves Crespin, patron de la Brigade d'enquêtes sur les fraudes aux technologies de l'information. Certains scammeurs se font passer pour une jeune fille qui veut venir en France, à qui il manque quelques centaines d'eu-

PHOTO : AFP/SIPA/SAUDAY ALAMBA

VIEUX COMME LE SCAM

Le scam n'est pas une nouveauté. A la fin du XVIIIe siècle, après la Révolution, des escrocs écrivaient des missives très ressemblantes aux mails envoyés aujourd'hui par les cyber-escrocs. La plupart du temps, ils se faisaient passer pour le serviteur d'un noble qui avait dû fuir et avait enterré une partie de ses biens au pied d'un chêne centenaire. L'arnaque a été remise au goût du jour dans les années 1980 au Nigeria, d'où l'expression de spam nigérian ou de fraude 419 – ce numéro correspond à l'article 4.1.9 du code pénal nigérian qui réprime ce genre de pratique. Au départ, les escrocs opéraient par courrier ou par fax. L'arrivée du mail a permis de réduire le coût du démarchage et de multiplier les prospects. Aujourd'hui, les cyberescrocs opèrent pour beaucoup depuis le continent africain, l'Asie ou encore l'Europe de l'Est.

la corde sensible



DANS UN CYBERCAFÉ DE LAGOS, au Nigeria, des placards avertissent les internautes des risques encourus s'ils sont pris en flagrant délit de spam ou de scam. Ces activités qui ternissent l'image du pays font l'objet d'une action résolue du gouvernement depuis quelques années.

ros pour payer son billet d'avion. Bien sûr, à son arrivée, cette dernière s'empressera de rencontrer son bienfaiteur, et plus si affinités.

Très peu d'arrestations

Les victimes de ces arnaques qui pullulent depuis la multiplication des boîtes mail se manifestent rarement. Beaucoup n'osent pas avouer qu'elles ont cru pouvoir s'enrichir facilement ou faire une rencontre à peu de frais. *"Elles viennent nous voir en général quand le préjudice atteint 15 000 euros ou plus"*, explique Yves Crespin. Cela explique en partie le faible nombre d'affaires qui finissent devant la justice. Il faut aussi souligner que les malfaiteurs restent la plupart du temps cachés derrière leur messagerie et ne se déplacent pas pour récupérer l'argent qui est expédié le plus souvent sous la forme de mandats. Ils opèrent principalement depuis l'Asie, l'Europe de l'Est ou encore l'Afrique, dans des pays où la lutte contre la cybercriminalité n'est pas une priorité. Les mails sont envoyés depuis des cybercafés. Difficile dans ces conditions pour les enquêteurs de retrouver les escrocs. *"Il arrive qu'on en coince certains quand ils se déplacent à l'étranger,* explique Yves Crespin, *mais cela reste relativement rare."* Le premier procès en France a eu lieu en septembre dernier, alors même que le scam existe depuis belle lurette, avant même l'invention du mail. L'arnaque a encore de beaux jours devant elle. D'autant plus que les escrocs perfectionnent leurs techniques d'approche. *"Depuis un an, on assiste*

LE "SCAM BAITING" OU COMMENT SE PAYER UN SCAMMEUR

Ils se surnomment eux-mêmes les "croque-escrocs". Leur ambition ? Arnaquer les scammeurs, ou tout au moins leur faire perdre du temps. Et nous faire rire par la même occasion. En anglais, cette pratique a un nom, le *scam baiting*. Elle prend plusieurs formes, du simple échange de mail avec l'arnaqueur au coup de fil ; certains cherchent même la rencontre ! Sur le site 419eater.com la bible du scam baiting, on trouve des exemples hallucinants des techniques mises en œuvre par ces antiscammeurs. Et c'est particulièrement drôle, puisqu'ils poussent souvent le vice jusqu'à demander à leur interlocuteur une photo de lui avec une pancarte ridicule ou une chaussure sur la tête. En français, le site "Mes amis les cyber-escrocs", animé par Julia Brandeau propose aussi de nombreux scams et contre-scams savoureux. En particulier cette rubrique qui recense des entretiens par chat entre des escrocs et... des robots de conversation !

à la montée en puissance d'une deuxième génération de scams", note Yves Crespin. Au lieu d'envoyer un mail standard à des milliers de personnes, les escrocs commencent à cibler leur victime. *"Ils vont par exemple sur les sites des ONG pour piocher les e-mails de personnes sensibles aux questions de solidarité, promptes à mettre la main au portefeuille pour aider les autres*, explique-t-il. *Ensuite, ils les contactent avec un mail personnifié, bien tourné."* Un exemple parmi les nombreuses variantes : Abdu, 11 ans, apprend le français à l'école et cherche une personne pour correspondre et l'aider à progresser. Pendant un mois ou deux, l'escroc va échanger des mails avec l'internaute qui a répondu, histoire de le mettre en confiance. Une fois le lien créé, il va commencer à lui soutirer de l'argent sous différents prétextes : acheter des livres pour aller à l'école, des médicaments pour une petite sœur malade... Les généreux donateurs reçoivent des mails de remerciement de la maman, de la grand-mère. *"Petit à petit, les escrocs inventent une famille virtuelle"*, résume Yves Crespin, qui s'inquiète du développement de cette nouvelle génération de pourriels plus ciblés, mieux ficelés.

Attention à la deuxième tournée !

Avec eux, il ne s'agit plus de faire miroiter monts et merveilles, mais de prendre l'internaute par les sentiments. Les scammeurs commencent d'ailleurs à écumer les sites et les chats de rencontre, à la recherche d'âmes sensibles. Il est ingénieur pour une firme pétrolière en Afrique. Après des années de bourlingue, il veut se poser, construire une famille. Bien sûr, il a de grosses économies. Évidemment, il aime les enfants, même ceux des autres. La correspondance dure quelques mois. Juste avant de rentrer au bercail, comme par hasard, l'homme a quelques problèmes de transfert d'argent vers son compte local. Il lui manque quelques milliers d'euros pour prendre son billet d'avion. Devinez qui va les lui avancer...

Les escrocs choisissent de mieux en mieux leurs victimes, mais aussi le moment propice pour passer à l'action. Quoi de mieux qu'une catastrophe naturelle pour apitoyer l'internaute et crédibiliser un appel au secours. *"Dès qu'il y a un séisme un peu important, un ouragan, dans les heures qui suivent, on voit partir les premiers scams"*, confirme Yves Crespin. Les scammeurs peuvent se faire passer pour une victime qui a tout perdu, un compatriote coincé sur place qui a besoin d'argent pour rentrer chez lui. Ils ne manquent pas d'imagination pour abuser de la crédulité des internautes qui se laissent prendre au piège. D'ailleurs, une fois qu'elles ont découvert le pot aux roses, les victimes ne sont pas à l'abri de se faire dépouiller une deuxième fois. Si la victime refuse d'aller plus loin, les escrocs laissent passer un peu de temps. Ils reprennent ensuite contact en envoyant un mail qui a l'apparence d'un courrier officiel, la plupart du temps en provenance du FBI. Ce dernier vient annoncer à la victime que les malfaiteurs qui l'ont dépouillée ont été arrêtés et qu'une procédure va être engagée contre eux au terme de laquelle elle pourra récupérer son argent. Pour porter plainte, elle doit impérativement prendre contact avec un avocat sur place qui suivra l'affaire. Et comme tout travail mérite salaire, il faut payer une avance à l'homme de loi. C'est le deuxième effet scam. *"Contrairement à ce qu'on pourrait penser, beaucoup de victimes se font avoir"*, explique Yves Crespin. Difficile en effet d'admettre qu'on s'est fait "bananer" et qu'on ne reverra pas son argent. Les scammeurs ont décidément bien assimilé les ressorts de l'âme humaine, il n'en sont que plus redoutables. • **N.Re.**

Spam: un vieux casse-pieds toujours vert

Publicités pour le Viagra, fausses montres ou crédits défiant toute concurrence... *Tout internaute a déjà reçu ces mails gênants, aussi vieux que l'Internet et encore loin de nous laisser en paix. À moins que...*

déjà 30 ans que le spam fait rage (*voir page 8*). Et si ces messages publicitaires non sollicités sont moins dangereux que les tentatives de phishing, ils n'en demeurent pas moins usants, surtout qu'ils ne cessent de trouver de nouveaux moyens de propagation. En mai dernier, d'après la firme Message Labs, le spam représentait 76,8 % du volume global des e-mails échangés sur Internet, un chiffre que l'on n'avait pas atteint depuis au moins un an. Et ce n'est pas tout. L'agence de sécurité européenne Enisa estime qu'il a coûté la bagatelle de 27 milliards d'euros à l'Union européenne, et 65 milliards aux entreprises de monde entier, soit deux fois plus qu'en 2005. Et ce malgré des filtres toujours plus efficaces : seuls 6 % des spams arrivent effectivement dans nos boîtes mails, mais étant donné que le spam grossit en quantité, en taille et donc en bande passante, il demeure un véritable fléau financier.

Faire barrage à la source

Et pourtant, certains estiment que le problème pourrait être en partie résolu si l'on s'attaquait aux sites de pub vers lesquels les spammeurs pointent. Début mai, le site spécialisé KnujOn dévoile un rapport hallucinant qui prouve que les sites Web où les internautes sont incités à se rendre sont presque tous enregistrés chez les mêmes fournisseurs de noms de domaine ! La démonstration qu'apportent ces spécialistes est simple : *"Par exemple, un botnet de 100 000 machines envoie une campagne de spam de 2 millions de messages. Le spam ne pointe en réalité que vers 200 à 500 URL, qui ne sont souvent que de simples redirections vers 100 à 200 domaines différents, dont 90 % sont contrôlés par 2,5 % des fournisseurs de noms de domaine. Donc beaucoup d'expéditeurs, beaucoup de messages, mais qui renvoient le troupeau de victimes vers un tout petit enclos."* CQFD. D'après ce rapport, seule une dizaine d'entreprises fourniraient l'essentiel des sites vers lesquels pointent les spammeurs.

Pub clandestine sur les services en ligne

Autrement dit, si on ne parvient pas à réguler l'expédition de spam, il pourrait être possible de supprimer les sites vers lesquels ils dirigent, ce qui mécaniquement, ferait baisser l'envoi de messages. À la suite de ce rapport, l'Icann, l'instance internationale qui gère l'attribution des noms de domaine, a réagi. Fin mai, elle annonce qu'il faut faire une différence entre un enregistreur de noms de domaines qui se serait fait berner par un utilisateur spammeur, et un fournisseur qui effectivement ne respecte pas les règles du jeu. Mais promet tout de même que s'ils ne se conforment pas aux règles, ils perdront leur droit d'enregistrer des noms.

Cela suffira-t-il ? Pas sûr. Car les spammeurs sont des gens pleins de ressources. Qui usent et abusent de chaque nouvelle technologie pour envoyer leurs satanés courriers. Les blogs sont pour eux du pain bénit, tout comme les espaces de commentaires ou les forums. Et leur tout nouveau terrain de jeu est plutôt prometteur : on constate en effet qu'ils s'attaquent désormais aux logiciels en ligne. Google Documents, le traitement de texte du géant de la recherche est ainsi devenu en l'espace de quelques mois une énorme base de données pour pourriels en tout genre. Pratique : les spammeurs n'envoient plus leur texte publicitaire, ils se contentent de publier leurs spams sur Google Docs et pointent vers eux dans leurs mails à l'aide d'un simple lien. Double avantage : les sites de spam sont, du coup, plus difficiles à repérer. • **E.L.B.**

UNION SACRÉE CONTRE LE SPAM PAR SMS

"Vous venez de gagnez un chèque. Rappelez vite le 08 XX XX XX XX pour en connaître le montant". Des messages qui frisent l'escroquerie pure et simple, vous en avez peut-être déjà reçu. Ils renvoient tous vers des numéros surtaxés qui peuvent faire mal lors du paiement de la facture. Luc Chatel, secrétaire d'État chargé de l'Industrie et de la Consommation semble décidé à nous débarrasser de ces menaces grandissantes. Il souhaite mettre en place rapidement un *"comité de déontologie des services de communication au public en ligne"*, qui réunirait pouvoirs publics, opérateurs et éditeurs de services. Ce groupe discutera des modalités techniques à mettre en place pour parer à ces pratiques intrusives.

Les entreprises : une

À part les grands groupes, rares sont les entreprises qui ont mis en place une architecture de sécurité efficace *pour protéger leurs données sensibles ainsi qu'une politique d'éducation en direction de leurs salariés. Les deux sont pourtant indispensables pour une protection réelle.*

Avril 2005. Une jeune Chinoise en stage chez l'équipementier automobile Valéo est arrêtée et mise en examen pour intrusion dans un système automatique de données. L'entreprise l'accuse d'avoir recopié des fichiers informatiques confidentiels *"sans rapport avec son stage"*. Lors de son procès, deux ans plus tard, la jeune fille plaidera la maladresse. Elle sera blanchie de toute accusation d'espionnage, mais écopera de deux mois de prison pour abus de confiance. Même si, au final, le préjudice est bien moins important que ce que Valéo avait laissé entendre au départ, l'affaire Li-li a mis en exergue la problématique de la sécurité informatique dans les entreprises.

> **"BEAUCOUP DE SOCIÉTÉS PRÉFÈRENT NE PAS PORTER PLAINTE PAR CRAINTE DE LA PUBLICITÉ NÉGATIVE.**

Valéo n'est pas le seul acteur économique à avoir vu des données partir dans la nature. Dans la majorité des cas, les entreprises préfèrent cependant rester discrètes. *"Les affaires arrivent rarement sur la place publique,* explique Christian Aghroum, qui dirige l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). *À notre grand regret, Beaucoup de sociétés préfèrent ne pas porter plainte. Elles ont peur que cela leur fasse une mauvaise publicité."* Il arrive aussi que les entreprises ne s'aperçoivent pas qu'elles ont été victime d'une attaque numérique. *"De temps en temps, nous faisons des expertises judiciaires sur des serveurs,* explique Hervé Schauer, consultant en sécurité informatique. *Il n'est pas rare qu'on découvre des traces d'intrusions passées inaperçues."* Souvent, les dirigeants commencent à s'intéresser à la sécurité quand il est déjà trop tard, une fois que le mal est fait. Vol de données de recherche et développement, de bases clients, atteinte aux personnes dirigeantes, à la disponibilité des ressources : le préjudice pour l'entreprise peut pourtant être très important. Dans certains secteurs où la concurrence internationale est vive, l'information est une denrée stratégique qui peut se monnayer très cher. Les pirates le savent. En janvier dernier, un mathématicien de 58 ans a été arrêté en Grèce. Il était recherché depuis 2002 à la demande de Dassault qui le suspectait d'avoir revendu un peu partout dans le monde des informations industrielles secrètes à près de 250 personnes et des copies du logiciel de conception d'équipements (automobile, aéronautique et militaire) du groupe aéronautique. Coût estimé pour Dassault : 361 millions d'euros.

proie trop facile ?

Face à cette menace grandissante, les entreprises commencent à réagir. Il était temps. La situation est préoccupante. Selon une enquête publiée par le Clusif fin 2006, seulement 56 % des entreprises sont dotées d'une politique de sécurité de l'information. La plupart des grands groupes, notamment ceux qui œuvrent dans des secteurs très concurrentiels, ont un responsable de la sécurité informatique chargé de mettre en place et de faire évoluer une architecture de sécurité. Par contre, les PME et les PMI sont beaucoup plus vulnérables. *"Pour elles, la sécurité reste un produit de luxe,* explique Hervé Schauer. *Elles ont souvent des problèmes plus importants à traiter au quotidien"*. La plupart se contentent d'installer un antivirus et un pare-feu sans aller plus loin.

Tout une culture à acquérir

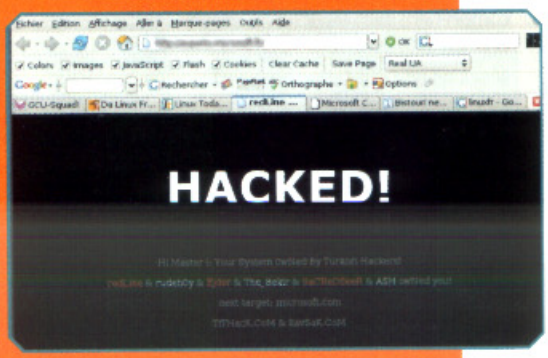
Il existe pourtant des grands principes à respecter si on veut être un tant soit peu tranquille. Il faut notamment veiller à cloisonner les serveurs, à installer des machines bastions devant servir de rempart aux attaques venant de l'extérieur. Nombreuses sont les entreprises qui n'ont engagé aucune démarche dans ce sens. *"Certaines ont des serveurs qui contiennent des données critiques directement connectés à Internet,* s'étonne Hervé Schauer. *Il n'est pas rare, par exemple, qu'il soit possible d'accéder à la base clients à partir de leur site."* Les failles sont multiples en général : logiciels mal programmés, systèmes mal configurés ou pas à jour, architectures mal conçues. Le problème ne doit cependant pas être être seulement appréhendé d'un point de vue technique. Pour que la protection soit efficace, il faut aussi qu'il y ait une véritable culture de la sécurité parmi les salariés. Si les utilisateurs ne respectent pas un certain nombre de règles, le système peut vite devenir une vraie passoire. Il n'y a pas que les prouesses techniques qui permettent d'aller fureter dans les dossiers confidentiels. Il suffit parfois d'un scénario bien monté pour récupérer un mot de passe et faire son marché. Les pirates sont aussi de bons psychologues. Souvent, au lieu d'attaquer directement le système, ils ciblent le maillon faible, à savoir l'utilisateur. Ils font ce que les spécialistes appellent de "l'ingénierie sociale". Avant de passer à l'attaque, ils recueillent des informations sur la société, l'organigramme, les logiciels utilisés, l'utilisateur qu'ils vont manipuler, de manière à le convaincre de donner des identifiants, d'ouvrir un fichier piégé ; en clair, de leur permettre, bien malgré lui, d'entrer dans le système de la boîte.

> *POUR LES PME ET PMI, LA SÉCURITÉ EST BIEN SOUVENT PERÇUE COMME UN PRODUIT DE LUXE*

Pour preuve, cette histoire relatée dans le livre *Cybercriminalité* écrit par le journaliste Philippe Richard et le spécialiste en virologie et cryptologie, Eric Filiol (*voir aussi page 52*). Un pirate ayant recueilli de nombreuses informations sur les salariés d'une société, les dossiers en cours, téléphone à l'administrateur système le jour où l'entreprise doit signer un contrat important. Il se fait passer pour l'ingénieur commercial responsable de la négociation et déclare qu'il n'arrive pas à se connecter sur l'ordinateur de la société alors que, évidemment, tous les documents importants se trouvent dessus : son mot de passe est soi-disant systématiquement refusé. Grâce aux informations recueillies et à une bonne dose de bagout, le pirate parvient à convaincre l'administrateur de changer le mot de passe. Fin de l'histoire : il ne lui reste plus qu'à se servir. • **N.Re.**

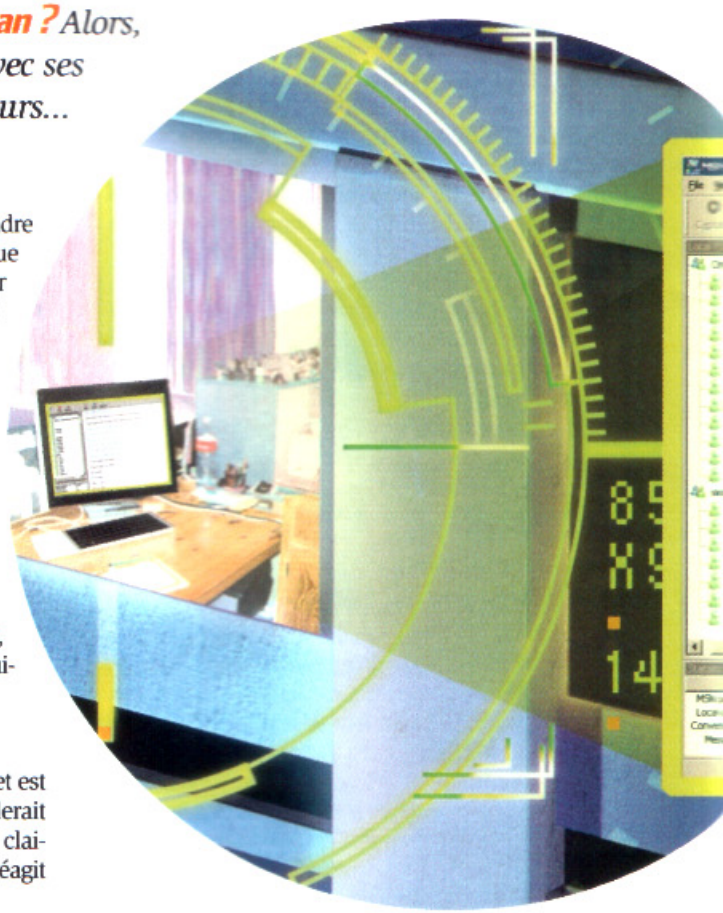
ATTENTION AUX COLLÈGUES...

On ne le dira jamais assez : la prévention des attaques et des intrusions passe par une sensibilisation accrue des salariés et l'acquisition de réflexes. Une simple clé USB peut faire des dégâts. Elle peut contenir un cheval de Troie qui va automatiquement s'installer sur la machine de l'utilisateur, un programme qui va aspirer du contenu... Pour éviter les accidents, une seule solution : expliquer, faire de la prévention. Les utilisateurs n'ont pas toujours conscience que leur comportement est "à risque". D'autant que la menace ne vient pas toujours de l'extérieur. En effet, la plupart des vols, des intrusions, sont le fait de personnes qui sont ou qui ont été dans l'entreprise : personnel mécontent, administrateurs système soudoyés, anciens salariés dont on n'a pas désactivé le compte utilisateur... Mieux vaut donc rester prudent, ne pas donner son mot de passe à tous les copains du service, ne pas laisser traîner trop de fichiers sur le Bureau, travailler dans les espaces protégés s'ils existent... Plus facile à dire qu'à faire entrer dans les mœurs. *"Contrairement à ce qu'on pourrait penser, ce sont souvent les cadres et les dirigeants qui contournent les consignes de sécurité"*, note Hervé Schauer. Un gros travail de sensibilisation reste à faire. *"Euh, patron, vous serait-il possible de fermer la session une fois que vous avez terminé... s'il vous plaît..."* Pas toujours facile d'être responsable de la sécurité en entreprise.



Ce que vos collègues sa

Salariés, vous vous croyez à l'abri derrière votre écran ? *Alors, gare ! L'entreprise est un réseau comme un autre, avec ses espions avides d'apprendre ce qui se trame en ses murs...*



Les salariés qui utilisent un ordinateur dans le cadre de leur travail pourraient être tentés de croire que son contenu est aussi privé que celui de leur machine personnelle, celle qu'ils utilisent à domicile. Lourde erreur ! Une méprise encore plus funeste si, comme c'est maintenant presque toujours le cas, ledit ordinateur est relié à un réseau local, voire à l'Internet. En effet, dans le cadre d'un réseau local d'entreprise, tous les ordinateurs sont reliés, par l'intermédiaire des prises et câbles muraux, à un ordinateur central, le serveur. La plupart du temps ces réseaux d'entreprise sont de type Ethernet. Un protocole répandu, relativement simple à maîtriser et peu coûteux à déployer, surtout depuis que tous les ordinateurs sont équipés de sa prise réseau typique, la RJ45.

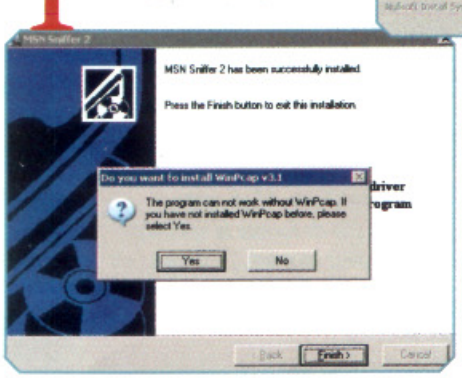
Épié de l'intérieur...

Or, dans sa version de base, le protocole Ethernet est l'équivalent d'une pièce où tout le monde parlerait chacun son tour à voix haute : chacun entend clairement ce que dit celui qui a la parole, mais ne réagit

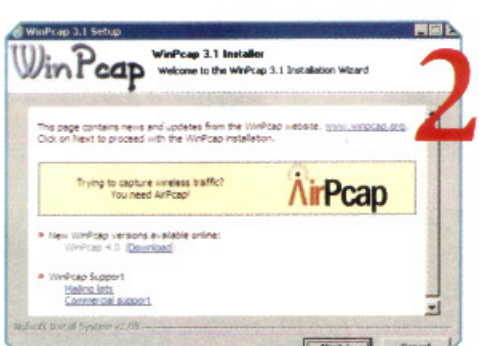
MSN Sniffer 2, rôder sur MSN avec de grandes oreilles

Les programmes qui capturent et reniflent les trames réseaux ramènent le plus souvent des tonnes d'informations, pas toujours compréhensibles ou utiles. C'est pourquoi certains se sont spécialisés dans une utilisation bien particulière. Une des plus prisées est le sniffage de MSN Messenger. Ces programmes présentent en clair toutes les discussions MSN qui passent sur le réseau local, avec une présentation agréable pour savoir qui dit quoi à qui. Tout pour espionner ! Il en existe plusieurs, et nous avons fait le test, à la rédaction, de MSN Sniffer 2, édité par Effetech. Son usage est relativement facile, sauf si votre réseau local est en Ethernet dit "commuté" (*voir encadré page suivante*). Il faut en premier lieu se rendre sur www.msnsniffer.com et télécharger une version d'évaluation. Après l'installation (1)– qui, dans la foulée, installe le pilote de capture WinPcap (2)–, il faut redémarrer. On lance MSN Sniffer, on se logue soi-même sur MSN (ça marche aussi avec Live Messenger), et on n'a plus qu'à regarder (3) : les conversations des autres postes de votre réseau entre eux, ou même avec des contacts extérieurs, vont s'afficher toutes seules sur votre écran ! Les contacts apparaissent au fur et à mesure que des conversations sont démarrées, avec un petit signal clignotant montrant les messages que vous n'avez pas encore lus... Très pratique pour savoir ce qui se dit sur vous ! Le problème, c'est que vous ne pourrez le répéter à personne...

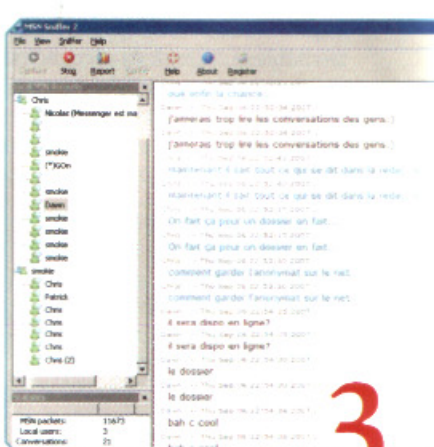
1



2



3



vent sur vous

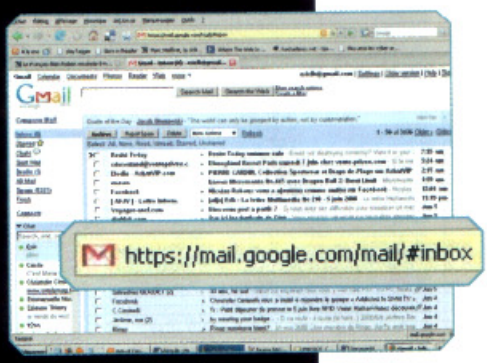
que quand il reconnaît qu'on s'adresse à lui. La carte Ethernet d'un PC fait exactement la même chose : elle écoute toutes les trames qui passent, mais ne retient que celles qui la concernent, oubliant les autres. Et c'est là qu'est la faiblesse du protocole : on peut, avec des logiciels spéciaux, capturer toutes les trames qui transitent sur le réseau, au lieu de les laisser tomber. Et la plupart du temps, tous ces paquets de données circulent en clair, sans aucun chiffrement. Dans ce fouillis d'octets, il est relativement facile d'isoler des textes, des mots de passe, ou encore le nom des sites Web visités par une personne.

Attention, donc, aux petits malins, voisins de bureau, qui peuvent installer sur leur PC ces fameux logiciels "sniffers", ou renifleurs : il n'est pas toujours besoin de pencher la tête par-dessus votre épaule pour savoir ce que vous faites tranquillement sur votre ordinateur en croyant être à l'abri des regards… Sachant que même si le salarié n'a pas le droit d'installer des programmes sur son ordinateur, il y a aussi la solution de démarrer sur un LiveCD Linux qui présentera lesdits outils sniffeurs.

Par ailleurs, toute entreprise possède son centre névralgique, via lequel transitent toutes les données : le, ou les serveurs. En théorie, il est sécurisé – logiciellement, bien sûr, mais aussi physiquement, par exemple dans une pièce dont seul l'administrateur réseau a l'accès. Il n'empêche : tout dépend de lui. Il règne sur ses serveurs et peut intercepter ou lire tout ce qui y passe – sous réserve bien sûr que les échanges ne soient pas chiffrés. Si le serveur est mal configuré ou mal tenu à jour, un utilisateur astucieux peut s'y introduire et regarder les fichiers et correspondances de ses collègues. Heureusement, les administrateurs sont en général des gens consciencieux. Consciencieux, mais aux ordres de la direction, ne l'oublions pas… • **N.R.**

COMMENT PRÉSERVER UN MINIMUM SA VIE PRIVÉE ?

- **CRYPTEZ, CRYPTEZ !** Le meilleur moyen pour écarter les regards indélicats de ce que vous envoyez sur le réseau est d'utiliser la cryptographie. Mais parmi les webmails, rares sont ceux qui proposent une connexion chiffrée de bout en bout. Avec Netcourrier, par exemple, tout circule en clair, même votre mot de passe. C'est pourquoi nous recommandons Gmail, avec l'astuce suivante : initiez la connexion en tapant dans la barre l'adresse https://gmail.google.com, sans oublier le "s" après http. Le petit verrou des pages sécurisées apparaît : dès lors, tout ce que vous recevrez et enverrez de Gmail sera protégé.

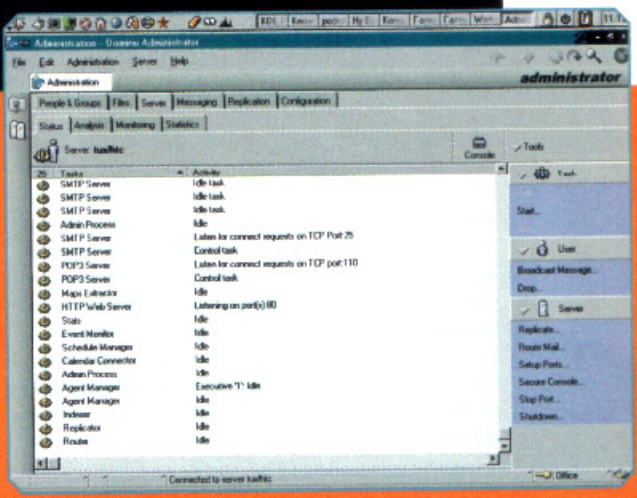


- **RESPECTEZ LA LOI.** L'article L.266-15 du code pénal protège la vie privée. En 2001, la Cour de cassation confirme que l'employeur ne peut pas prendre connaissance des messages personnels du salarié sans violer sa vie privée. Il y a donc une tolérance sur le lieu de travail, mais qui ne doit malgré tout pas nuire à l'entreprise ou à la bonne exécution du travail. Enfin, tout fichier ou dossier présent sur le PC de l'employé est présumé être professionnel, sauf s'il est explicitement marqué comme personnel. C'est un arrêt de la Cour de cassation de 2006 qui le précise.

- **PASSEZ LE RÉSEAU LOCAL EN MODE COMMUTÉ.** Ce type de réseau Ethernet est nettement plus sécurisé, car les PC ne reçoivent que les paquets qui leur sont explicitement destinés, ce qui limite les risques d'écoute par un collègue trop curieux. Aujourd'hui, la plupart des réseaux locaux sont de type commuté. Des techniques existent pour les espionner, mais elles sont plus dures à mettre en œuvre.

ADMINISTRATEUR RÉSEAU : L'ŒIL DE L'ENTREPRISE

Dans un réseau d'entreprise, l'administrateur réseau est en position stratégique : tout passe par les serveurs dont il a la garde. Frédéric Pognant, administrateur réseau dans un grand groupe de presse, confirme bien que *"toutes les demandes de visites sur un site, par qui et quand, tout est enregistré comme historique. On est le premier fournisseur d'accès à Internet de nos utilisateurs ! Mais on se limite à la sécurité, pour détecter les activités anormales comme un client peer-to-peer qui mange toute la bande passante"*. Quant aux mails, il peut aussi voir tout ce qui entre et sort : *"Je peux physiquement le faire, mais la loi et l'éthique l'interdisent. Et en plus j'ai autre chose à faire !"*



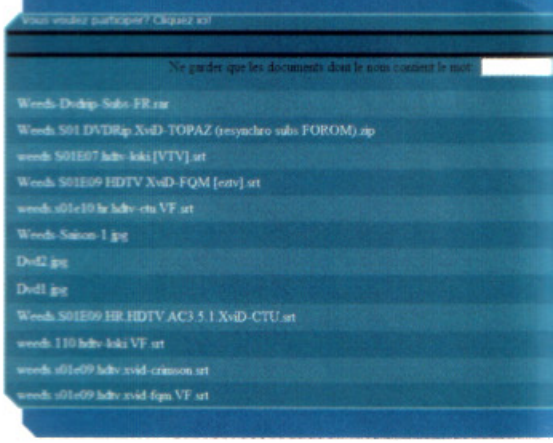
Qui se cache derrière les

Les contenus illégaux sur Internet sont tous les jours plus nombreux. *Mais qui donc les fournit ? Il y a évidemment de simples internautes, mais surtout des cercles organisés de véritables experts.*

Les crackers Des spécialistes qui copient les jeux vidéo et les logiciels

Ils hantent les cauchemars des éditeurs de jeux et de logiciels. Leur spécialité : permettre de lancer des copies d'un logiciel original à partir de l'image du programme ou d'un disque gravé. Ils sont particulièrement actifs dans le jeu vidéo, notamment sur PC, les plus fréquents sur Internet. Concrètement, le cracker, fin programmeur, analyse le code source du jeu, trafique les fichiers qui activent la protection mise en place par l'éditeur, et propose, avec la copie du jeu, les fichiers qu'il a modifiés.

Les créateurs de Des pros de la traduction



Tous les jours, des milliers de nouveaux contenus piratés atterrissent sur Internet. Films, jeux, logiciels, disques, cette grande foire ne s'arrête jamais. Les principaux fournisseurs, on les connaît bien, ce sont les mêmes depuis l'émergence de Napster : de simples internautes qui, pour une raison ou une autre, décident de partager ce qu'ils possèdent avec la communauté. Des raisons assez obscures, parfois, qui poussent par exemple des centaines de "posteurs" sur les forums Usenet à découper des films DivX qu'ils ont au préalable encodés depuis un DVD ou récupérés ailleurs sur Internet, puis qu'ils ont coupés en dizaines de morceaux pour qu'ils puissent être codés comme messages sur ce système d'échange aujourd'hui obsolète. Et qui doivent par-dessus le marché leur appliquer un système de correction d'erreur pour être bien certains que le téléchargeur de l'autre côté puisse le récupérer sans encombre. Un long travail de piratage… Sans compter que, parfois, ces "posteurs" prolifiques se donnent même la peine d'enregistrer le film directement dans la salle de cinéma, pour être les premiers à le proposer sur les différents services Internet.

Être le premier à "offrir" un contenu : voilà sans doute leur principale motivation. Sur Usenet comme sur les services P2P, l'ego de ces fournisseurs illégaux est clairement mis en avant. En témoignent leurs commentaires, souvent très personnels, à propos du fichier qu'ils proposent. Cela va de la déclaration d'amour à leur petite amie aux jugements définitifs du type *"bidule vous offre le meilleur film de tous les temps"*. Ils sont d'ailleurs souvent chaudement remerciés par ceux qui en ont profité.

Pirates d'eau douce ou du grand large

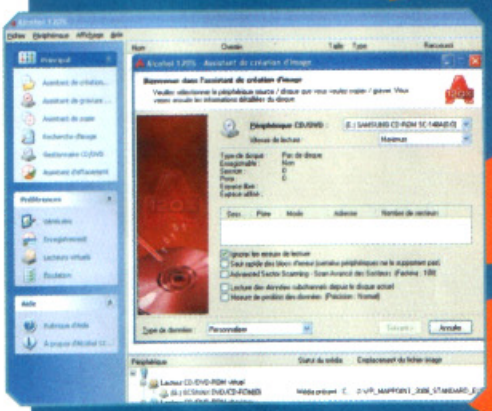
C'est bien joli, mais assez "petit joueur" comparé à d'autres fournisseurs de ce Web interdit qui ne cesse de grossir. Si les P2Pistes ont un peu volé la vedette aux pirates qui proposaient, bien avant Naspter, des contenus illégaux en avant première, ils ne sont pas à même de remplacer ces spécialistes de la rapine, bien renseignés, parfaitement organisés et, pour certains, capables de casser la sécurité de la plupart des logiciels pour en faire profiter gratuitement le plus grand nombre. Business ou défi technique, les raisons qui poussent au "crack" varient. Mais la plupart des contenus illégaux qui traînent sur le Net proviennent en réalité de ces nombreux groupes qui constituent l'élite du piratage et se surnomment "La Scène". Spécialisés dans un type de contenu ou une plateforme, ils sont les premiers à récupérer et à profiter des films, jeux ou musiques... avant même

contenus illicites ?

Fan-sub
pour les vidéos étrangères

Énorme travail que celui des amateurs de Fan-sub, discipline qui consiste à ajouter des sous-titres "amateurs" à une vidéo en langue étrangère, pas encore sortie dans le commerce en France. Le Fan-sub est très fréquent chez les amateurs de séries télévisées. Ces pros de la traduction ne prennent en général que quelques jours pour mettre en ligne les dialogues d'un nouvel épisode, qu'ils doivent traduire de façon honnête et synchroniser avec le fichier DivX de la bande vidéo.

Les programmeurs Ils conçoivent les logiciels utiles au piratage



Ils développent des programmes qui participent au piratage. Des logiciels comme Deamon Tools ou Alcohol, bien que disponibles aisément sur le Net, sont majoritairement employés par qui veut faire tourner un jeu téléchargé sur sa machine : ils sont en effet capables de faire passer une copie pour un disque original, et émulent par ailleurs les protections des jeux vidéo. Des logiciels comme cela, il y en a à la pelle, pour la gravure, l'émulation, ou le détournement des DRM.

Les partageurs Ils mettent leurs contenus à la disposition de tous

Eux n'ont pas de compétence technique particulière : ils mettent des contenus à la disposition d'autres internautes, contenus qu'ils ont parfois eux-mêmes encodés. Ils sont très nombreux à partager de la musique, plus rapide et facile à distribuer que le reste. Ils ont fait la gloire du P2P, mais sont en moins grand nombre aujourd'hui : les procès contre certains d'entre eux ont un peu appauvri les réseaux classiques. BitTorrent cartonne, soit, mais il est plus complexe de mettre en place un partage avec ce protocole.

PARTIS PIRATES

POUR UN INTERNET OUVERT ET LIBRE

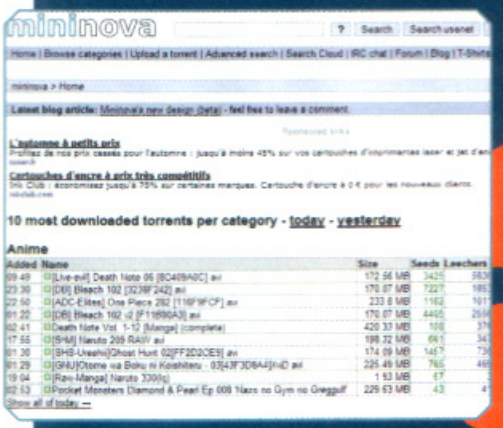
LES MILITANTS POUR LA CULTURE GRATUITE ONT DÉCIDÉ DE SE FAIRE ENTENDRE SUR LA TOILE FRANÇAISE.

Sous le nom de Parti Pirate Français, ils diffusent leur programme radical : abolir le droit d'auteur, autoriser l'anonymat sur le Net, ouvrir l'accès aux œuvres numériques sans contraintes et permettre leur libre partage, supprimer la taxe sur les supports vierges, instaurer la gratuité de l'accès au Net... On peut sourire. Eux, comptent peser sur la campagne électorale et prévoient de rédiger un argumentaire sur chaque candidat selon le sort qu'il réserve aux internautes. Les Suédois leur servent de modèle : ThePirateBay est un phénomène très influent auprès des jeunes, et le Parti Pirate Suédois auquel il est lié possède de vrais moyens d'action. Il a, en outre, lancé un service pour surfer anonymement et télécharger sans se faire repérer, pour financer ses activités politiques (*SVM* n° 252 p. 33) !

Liberté • Égalité • Fraternité
PARTI PIRATE FRANÇAIS

Les fournisseurs d'accès à Usenet

Ils vendent le sésame pour pirater les newsgroups



Impossible de pirater correctement sur les newsgroups sans prendre un abonnement chez un fournisseur d'accès à Usenet. Nombreuses sont les sociétés américaines à proposer ce service contre dollars sonnants et trébuchants. Elles n'ont pour l'instant jamais été dérangées par les défenseurs des ayants droit... Contrairement à de nombreux webmestres qui ont mis en place un tracker BitTorrent (comme ThePirateBay), indispensable portail pour accéder aux contenus piratés avec ce protocole P2P.

leur sortie dans le commerce. Les œuvres qu'ils ont piratées "glissent" ensuite vers l'IRC (Internet Chat Relay, un protocole de discussion sur Internet), les newsgroups, les réseaux P2P, voire le Web. Tous ne sont pas des génies de l'informatique : en général, au moins un membre du groupe dispose d'un accès privilégié aux contenus, par exemple parce qu'il travaille chez un distributeur qui obtient jeux, musiques ou DVD quelques jours avant leur sortie officielle. Il le confie alors aux experts, qui vont s'occuper de transformer un film en DivX, de "ripper" un disque ou de craquer la protection d'un logiciel, avant de le distribuer. Exemples récents : *War Inc.* une comédie américaine, pas encore en salles en France... Ou encore le fameux jeu Assassin's Creed, disponible avant même sa sortie sur les réseaux P2P.

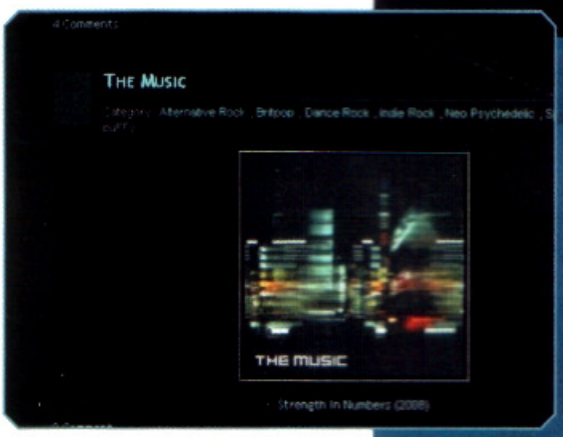
Programmeurs "pousse-au-crime"

Cela nous amène à évoquer d'autres fournisseurs de l'Internet underground. Eux ne fournissent pas de contenus, mais des programmes, parfois aux frontières de la légalité, voire carrément illicites. C'est le cas de tous ces logiciels qui permettent d'outrepasser les DRM conçus par Apple ou Microsoft pour protéger les fichiers musicaux, à l'image de FairUseWM, écrit par un hacker isolé qui a défrayé la chronique, en septembre 2007, en rendant obsolète l'écosystème PlayForSure de Microsoft. DVD Jon (*voir nos portraits page 14*) a plusieurs fois fait la même chose avec la protection FairPlay d'Apple, et encore tout récemment avec son nouveau service DoubleTwist. Celui-ci sert à partager des fichiers entre amis, et supprime au passage toutes les protections DRM des fichiers achetés sur iTunes. Quant aux programmes pour faire sauter les protections des jeux et logiciels, on les trouve facilement sur n'importe quel réseau P2P ou sur des sites du type RapidShare, ce qui amplifie grandement le nombre de contenus illégaux sur la Toile. • **E.L.B.**

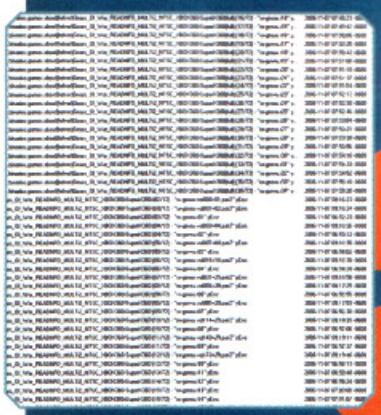
BLOGS MUSICAUX

LE NOUVEAU REPAIRE DES TÉLÉCHARGEURS

ILS SONT À LA POINTE DES DERNIÈRES TENDANCES MUSICALES et n'ont qu'une envie : en faire profiter un maximum de monde... Et pourquoi pas se faire de menus revenus publicitaires grâce à la pub qu'ils incorporent à leur site. Eux, ce sont les bloggeurs musicaux qui proposent, en téléchargement, des albums entiers... Pas tous, loin de là : la plupart des blogs musicaux se contentent d'héberger un ou deux fichiers MP3 d'un groupe donné, et encore, quelques jours seulement, pour faire découvrir sa musique aux visiteurs. Mais il existe aussi tout un univers de blogs bien moins respectueux des artistes. Eux n'hésitent pas à poster chaque jour plusieurs albums entiers, souvent parmi les sorties les plus récentes. Pour cela, ils passent pas un hébergeur tel que Rapidshare.com, très populaire. Pour les pirates, ces blogs représentent peut-être le plus grand eldorado depuis Napster car ils offrent des téléchargements ultraciblés.



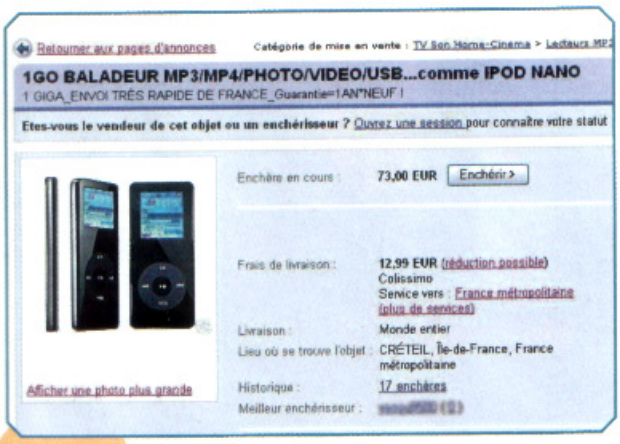
Les "privilégiés" Des partageurs de musique ou de films en avant-première



Ce sont des partageurs un peu spéciaux, qui ont eu accès avant tout le monde à un contenu et qui le partagent sur le Net. Ils font souvent partie d'équipes de pirates, mais agissent également seuls parfois, histoire de se faire mousser. C'était assez courant pour les films, mais depuis que les studios ont cessé d'envoyer des screeners (DVD de films sur le point de sortir ou encore en salle) aux professionnels du cinéma, l'offre a sérieusement baissé. En revanche, nombre de disques se trouvent propulsés sur le Net par ce biais avant leur commercialisation.

Gare aux contrefaçons !

Dans un marché de la contrefaçon en plein essor *(5 à 9 % du commerce mondial selon l'OCDE), la vente de copies en ligne n'a pas échappé à la tendance, surtout sur les sites d'enchères. Petit tour d'horizon des produits qu'il vaut mieux acheter chez un commerçant de confiance.* • **Par Nicolas Reynaud**



IPOD : LES FAUX JUMEAUX

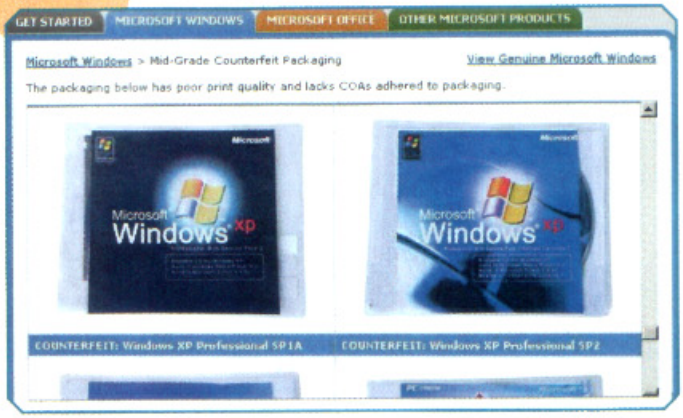
On trouve sur Internet des copies conformes du baladeur vedette d'Apple, à un prix imbattable. *"Ce ne sont pas à proprement parler des contrefaçons. Il n'y a pas la pomme. Le packaging est différent. Par contre, le design est le même*, note Lionel du site MacBidouille. *C'est de l'extrême inspiration"*. Sur eBay, la plupart des vendeurs qui proposent ces copies dans la rubrique iPod préviennent les acheteurs. Le procédé reste cependant contestable. En février dernier, Apple a fait condamner une société française qui distribuait ces clones.

Des placebos inefficaces ou dangereux

Coupe-faim, antidépresseurs, somnifères et bien sûr Viagra... Qui n'a pas reçu des spams en provenance d'officines obscures proposant ces produits ? Installées à l'étranger, la plupart des pharmacies du Web n'hésitent pas à vendre des médicaments sans ordonnance, voire des produits qui n'ont pas obtenu d'autorisation de mise sur le marché. Non seulement il peut être risqué de prendre ces pilules d'importation sans suivi médical, mais en plus, dans près de la moitié des cas, ces médicaments sont des faux pouvant contenir des produits dangereux pour la santé.

Le logiciel pirate

La copie pirate de logiciel est particulièrement difficile à détecter. Les contrefacteurs sont capables de reproduire les DVD d'installation, l'emballage (*capture ci-dessous*), les certificats d'authenticité. L'an dernier, les autorités chinoises ont démantelé un réseau de contrefacteurs qui avaient écoulé 5 à 6 millions de copies illicites de Windows dans près de 27 pays.



La batterie qui fait BOUM

L'Association internationale des fabricants de matériel photo et vidéo a lancé une alerte récemment : beaucoup de batteries Li-on et de chargeurs vendus sur les sites d'enchères sont des produits contrefaits. Le packaging est en général similaire à celui des produits de marques. Seuls quelques détails peuvent trahir la provenance douteuse de la marchandise, qui peut s'avérer dangereuse de surcroît : une batterie contrefaite peut chauffer, couler voire exploser.

LE LUXE À PRIX DISCOUNT

Comment reconnaître un vrai sac Vuitton d'un faux à partir d'une photo sur Internet ? Distinguer un vrai foulard Hermès d'une pâle copie ? Une Rolex bling bling d'un modèle toc toc ? Le prix peut-être... Certains consommateurs font semblant de ne rien voir et se laissent séduire, au grand dam des marques de référence qui commencent à se préoccuper du foisonnement de clones sur les sites d'enchères. Le groupe LVMH, numéro un mondial du luxe, propriétaire des marques Dior et Vuitton, a entamé une action en justice contre eBay en 2006. Il réclame 37 millions d'euros de dommages et intérêts au site d'enchères.

Attention,

Les États utilisent déjà les techniques du hacking pour faire du renseignement, *voler des informations stratégiques. Aujourd'hui, rien ne les empêche de s'en servir pour déstabiliser un adversaire.*

En 2007, plusieurs affaires ont montré combien la sécurité des réseaux d'information est en train de devenir un enjeu important pour les États. Plusieurs pays ont accusé la Chine d'avoir attaqué des sites stratégiques. Les hackers qui auraient été téléguidés par l'Armée populaire de Chine ont volé une centaine de gigaoctets de données au ministère des Affaires étrangères allemand. Ils ont récupéré les mails du Secrétaire à la défense américain, Robert Gates. En France, officiellement, l'attaque contre le ministère de la Défense n'a pas eu de conséquences graves. La Grande muette a préféré minimiser l'événement.

Pourtant, l'heure n'est plus à l'intimidation ou aux simples prouesses techniques. Avec la mondialisation et le développement de la concurrence qu'elle entraîne, le hacking est devenu un instrument du renseignement, un outil de la guerre économique. Il peut aussi être une arme en cas de conflit plus ou moins déclaré. L'année dernière, l'Estonie a dû faire face pendant plusieurs semaines à des attaques de déni de service répétées contre ses institutions publiques, ses banques, ses entreprises, suite au déplacement d'un mémorial à la gloire des soldats soviétiques dans le centre-ville de Tallinn, la capitale du pays. Pour combattre ces attaques, L'Estonie n'a pas eu d'autre solution que d'isoler le pays d'Internet pendant 2 jours. Le gouvernement, qui a mis en cause la Russie, a même demandé l'intervention de l'Otan. Une réaction peut-être disproportionnée mais qui traduit à quel point le développement de l'informatique et la numérisation de l'économie engendrent de nouveaux risques pour les États et les entreprises.

Vers la guérilla informatique ?

"On peut déstabiliser un pays en détenant des informations secrètes, en s'en prenant à des infrastructures stratégiques ou à son système bancaire", note Joël Ferry. Les cibles et les moyens sont différents de ceux d'un conflit traditionnel, mais le résultat final recherché reste identique : créer le chaos. Le conflit du futur sera, à n'en pas douter, une combinaison d'attaques conventionnelles et informatiques. Les réseaux d'eau, les barrages, les centrales élec-

cyberguerre en vue

triques, les systèmes de détection d'incendie, de gestion des transports collectifs sont contrôlés par informatique. *"Or, les systèmes propriétaires sont de plus en plus rares,* explique Hervé Schauer, consultant en sécurité informatique. *Beaucoup de systèmes sont construits avec des produits 'sur étagère', des protocoles connus de tous comme Ethernet ou TCP/IP. Cela ne peut que faciliter la tâche des pirates."* La paralysie pendant plusieurs heures des réseaux de surveillance d'une centrale nucléaire américaine en 2003, suite à la contamination par le ver Sapphire/Slammer, a mis en lumière la vulnérabilité des réseaux informatiques de nombreuses infrastructures civiles. Le problème est d'autant plus sérieux que la banalisation de l'informatique et la simplification des outils de hacking, ne font qu'accroître les risques d'agression. La menace devient plus diffuse.

Les attaques peuvent être menées par des États mais aussi des groupes de terroristes ou de militants. *"Dernièrement un groupe baptisé Anonymous a lancé une attaque coordonnée contre les serveurs de l'église de scientologie en fédérant des internautes sur le Web*, explique Laurence Ifrah, chercheuse au département de recherche sur les menaces criminelles contemporaines de l'université Panthéon-Assas Paris II. *Cela préfigure l'usage que pourraient faire des technologies des groupes mal intentionnés. Des organisations terroristes comme Al Qaeda s'intéressent de près à la question. Certaines ont recruté des techniciens de bon niveau parmi leurs rangs. Des islamistes radicaux ont développé, par exemple, des logiciels de cryptage de données qu'on ne sait pas cracker. La menace est bien réelle."* • **N.Re.**

> *"LE CONFLIT DU FUTUR SERA UNE COMBINAISON D'ATTAQUES CONVENTIONNELLES ET D'ATTAQUES INFORMATIQUES*

Trois questions à Laurence Ifrah

Laurence Ifrah est chercheuse au département de recherche sur les menaces criminelles contemporaines de l'université Panthéon-Assas, Paris II, et consultante en sécurité informatique.

SVM : Quelle place occupent les nouvelles technologies aujourd'hui dans le renseignement ?

Laurence Ifrah : Nous ne sommes plus dans la phase expérimentale. Les attaques qui ont été médiatisées ne sont que la partie émergée de l'iceberg. On a beaucoup parlé de la Chine mais tous les États espionnent, collectent des renseignements par le réseau Internet, les Américains les premiers, ce qui ne les empêche pas de protester vivement quand ils se font attaquer. Il y a une dizaine d'années, on comptait peut-être vingt personnes capables de monter des attaques ciblées. Aujourd'hui, on est bien incapable de dénombrer les hackers assez compétents pour s'en prendre à des réseaux sécurisés. Les militaires ont pris conscience du pouvoir de la technologie et travaillent sur des scénarios d'attaque informatique.

SVM : Que vont chercher les États ?

L. I.: Des renseignements militaires, bien sûr, mais aussi des informations sur des sujets sensibles comme la recherche médicale, le nucléaire, l'énergie. Souvent, les visées sont économiques. Certains pays comme la Chine, par exemple, ne cachent pas que la collecte de renseignements fait partie intégrante de leur stratégie industrielle. On ferait bien de se soucier un peu plus de la sécurité de nos entreprises.

SVM : Comment opèrent-ils ?

L. I.: Les services de renseignement et les gouvernements vont recruter des techniciens de haut vol dans les écoles d'informatique, mais aussi parmi les hackers. Certains États font faire le sale boulot à des groupes plus ou moins suspects, de façon à ne pas être impliqués directement. En échange des services rendus, ils ferment les yeux sur des activités louches. Quand il y a eu l'attaque contre l'Estonie, le Kremlin a fait savoir qu'il n'y était pour rien. De fait, les attaques ont été coordonnées par le Russian Business Network, un groupe de cybercriminels qui avait pignon sur rue à St-Petersbourg. C'est lui qui a loué les réseaux de botnet et mis à disposition les outils de hack sur les forums. Les services russes ne sont pas intervenus directement, c'est vrai. Au mieux, ils ont laissé faire, au pire, ils ont passé commande...

Du renfort pour la

***La criminalité et la délinquance sur Internet se développent** au même rythme que le Réseau. Michèle Alliot-Marie, ministre de l'Intérieur, a annoncé une série de dispositions pour endiguer le phénomène et permettre aux enquêteurs de lutter à "armes égales".*

L'État veut rattraper son retard, ou du moins ne pas se laisser distancer. En présentant mi-février 2008 son plan de lutte contre la cybercriminalité, Michèle Alliot-Marie a souligné qu'elle comptait bien donner les moyens aux enquêteurs de lutter à armes égales avec ceux qui bafouent la loi sur Internet.

Pourquoi cette sortie ? *"Parce que la délinquance et la criminalité sur la Toile ont beaucoup évolué ces dernières années"*, explique Christian Aghroum, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Avec le développement du haut débit, Internet est devenu une vaste aire de jeu où l'on retrouve toutes les composantes de la société, y compris les délinquants et les voyous. Trafiquants, proxénètes, contrefacteurs, pédophiles, terroristes et escrocs se servent du Web pour communiquer, échanger ou diffuser des informations, développer leur "business", extorquer de l'argent aux internautes un peu trop crédules… En plus de ces populations qui utilisent le Réseau comme terrain d'action, les enquêteurs doivent aussi traquer les pirates qui fomentent des attaques contre les sites et les systèmes de traitement automatisé des données. Vol d'identifiants bancaires (généralement par la technique du phishing, *voir page 22*), de bases de données, de secrets de fabrication, le cambriolage virtuel est en pleine expansion. Sont visés les particuliers mais aussi les entreprises, parfois même les États. *"Les bandes organisées se sont emparées des outils du hacking pour mener des attaques de grande ampleur, de plus en plus sophistiquées*, explique Pascal Lointier, président du Club de la sécurité de l'information français (Clusif). *On trouve désormais des chevaux de Troie construits sur mesure, des malwares adaptés au niveau linguistique selon la région visée."* Difficile d'évaluer précisément l'ampleur des dégâts, d'autant que de nombreuses victimes ne portent pas plainte. Au final, les sommes en jeu peuvent cependant être très importantes. Une attaque de phishing d'envergure peut ainsi rapporter plusieurs centaines de milliers d'euros.

Le chiffre

14 465

C'est le nombre de sites Web pédopornographiques signalés par les internautes en 2007

Un dispositif un peu daté

Pour traiter toutes les affaires où les nouvelles technologies jouent un rôle, la gendarmerie et la police disposent aujourd'hui de cinq cents enquêteurs spécialisés répartis dans les différents services et sur tout le territoire. La ministre de l'Intérieur veut doubler les effectifs et remettre à plat une organisation qui a vieilli prématurément. Elle souhaite dans un premier temps renforcer le rôle de l'OCLCTIC, qui mène des enquêtes d'envergure nationale et internationale ou intervient en renfort quand une expertise en matière de nouvelles technologies de l'information est nécessaire, et qui assure par ailleurs la formation des enquêteurs spécialisés et s'occupe de la coopération internationale. Les effectifs passeront de huit à une cinquantaine d'enquêteurs. Un groupe dédié aux escroqueries sur Internet sera créé. La plate-forme de signalement des sites pédophiles, lancée en septembre 2006, sera étendue à l'ensemble des délits à la rentrée prochaine. Le but est de faire remonter l'information plus

Le plan Alliot-Marie contre la cybercriminalité

- **Le doublement du nombre d'enquêteurs spécialisés.**
- **Le renforcement de la formation avec la création d'un cursus de spécialisation au sein de la police nationale.**
- **L'extension de la plate-forme de signalement mise en place pour les sites xénophobes ou pédopornographiques aux sites de propagande terroriste et à l'escroquerie en ligne.**
- **La possibilité pour les policiers de capter à distance des données informatiques.**
- **La création d'un site Internet de conseil et de prévention contre les contenus illicites pour sensibiliser les internautes.**
- **L'obligation pour les FAI et les hébergeurs de conserver les données de connexion, de façon à pouvoir identifier tout créateur de contenu en ligne.**
- **La création d'un délit d'usurpation d'identité sur Internet, passible d'un an d'emprisonnement et de 15 000 € d'amende.**
- **Le renforcement de la coopération internationale.**

police du Net

"Le piratage doit faire l'objet de sanctions spécifiques. Je proposerai la création de peines alternatives de travaux d'intérêt général pour les hackers."

Michèle Alliot-Marie, ministre de l'Intérieur

vite et de centraliser les plaintes des victimes comme c'est le cas aujourd'hui pour la pédopornographie. Une même escroquerie peut toucher des personnes habitant aux quatre coins de la France. Mieux vaut que l'affaire soit prise en charge par une brigade spécialisée pour éviter les démultiplications d'enquêtes et les pertes de temps. Mais la ministre veut aussi renforcer l'effort de formation à la base. *"On ne peut plus se contenter de faire reposer le dispositif sur des enquêteurs hyperspécialisés,* note Christian Aghroum. *Il faut inverser la tendance, étendre la compétence."*

Car à côté des affaires complexes liées à l'espionnage, au terrorisme ou au crime organisé, se développe une délinquance de proximité : arnaques artisanales, affaires de diffamation, d'usurpation d'identité. La saga des photos volées de Laure Manaudou n'est pas un fait isolé, les atteintes à la vie privée sont de plus en plus fréquentes. Pour pouvoir travailler plus efficacement, les enquêteurs réclament aussi des évolutions juridiques. La ministre a annoncé la création d'un délit d'usurpation d'identité passible d'un an de prison et de 15 000 € d'amende. La loi d'orientation et de programmation sur la sécurité intérieure en préparation devrait aussi autoriser la police à mettre des ordinateurs sous surveillance à l'aide de logiciels espions, dans le cadre d'affaires criminelles graves comme le terrorisme, la pédophilie, le crime organisé… La mesure n'est pas encore actée, mais elle est déjà controversée.

Quelles données conserver ?

Autre disposition qui fait l'objet de nombreuses critiques : la conservation des données. Un projet de décret obligeant les opérateurs de communication, les FAI et les hébergeurs à conserver des données liées aux contenus, avait suscité de nombreuses oppositions à l'époque du gouvernement Villepin. La ministre de l'Intérieur revient avec un projet similaire, au risque de déclencher une nouvelle levée de boucliers. Le décret en préparation, que s'est procuré le journal économique *Les Échos*, demande aux opérateurs et hébergeurs de conserver toutes les données susceptibles d'identifier un créateur de contenu en ligne : adresse IP, mot de passe, nom d'utilisateur, pseudonyme, terminal utilisé, coordonnées de la personne physique ou morale… L'obligation ne se limite plus aux seules données de connexion qui, elles, devront être conservées pendant un an par les cybercafés conformément à la loi "Lutte contre le terrorisme" de janvier 2006. Autant dire que la polémique ne fait que commencer. Que faut-il garder ? Jusqu'où l'État peut-il aller pour assurer la sécurité des citoyens

INTERVIEW

Le commissaire Yves Crespin dirige la Brigade d'enquête sur les fraudes aux technologies de l'information (Befti), chargée pour Paris et la petite couronne des affaires de piratage, de spam, de vol de données et de contrefaçon de logiciels.

"Des arnaques plus ciblées, plus intelligentes"

SVM Quel est le profil des contrevenants à qui vous avez affaire ?

Yves Crespin Nous avons tous les cas de figure : le salarié qui part avec le fichier clients quand il est remercié, le hacker qui s'introduit sur le serveur d'une entreprise pour voler des données ou faire du chantage, les escrocs qui utilisent l'e-mail pour soutirer de l'argent aux internautes crédules, le boursicoteur qui a acheté un logiciel contrefait...
Dernièrement, nous avons même arrêté un adolescent de 13 ans qui avait planté un site de jeux après s'en être fait exclure par le webmaster. Cela va vraiment de l'amateur qui a glané quelques outils sur Internet au professionnel qui a une vraie connaissance technique et qui l'utilise à des fins frauduleuses.

SVM La ministre de l'Intérieur vient d'annoncer un renforcement de la lutte contre l'escroquerie en ligne. Quelle était l'urgence d'un tel dispositif ?

Y. C. Tout le monde a reçu un jour ou l'autre un de ces e-mails qu'on appelle les scams, dans lesquels quelqu'un sollicite une aide pour virer une grosse somme d'argent, pour se faire soigner... La manœuvre commence à être connue. Cependant, nous assistons depuis quelques mois à l'émergence d'une nouvelle génération de scams plus ciblés, plus intelligents. Les escrocs récupèrent des adresses e-mails valides sur les sites des ONG, notamment dans les livres d'or. Ils envoient alors un mail personnalisé. Au départ, c'est assez anodin. Ils se font passer pour un enfant africain qui souhaite correspondre en français pour améliorer son orthographe, sa grammaire. Après plusieurs échanges, ils commencent à demander de l'argent pour aller à l'école, pour un membre de la famille qui est malade... Ils jouent sur la corde sensible. En général, quand les victimes arrivent chez nous, elles ont déjà perdu entre 10 000 et 15 000 €. Le problème, c'est que nous avons peu de moyens d'action. Les scammeurs opèrent généralement depuis l'Afrique et viennent rarement en Europe.

SVM Quelle est la proportion d'affaires pour lesquelles il est nécessaire d'enquêter à l'étranger ?

Y. C. Deux dossiers sur trois finissent à l'international. C'est la limite de notre action. Il faut vraiment qu'il y ait un gros préjudice pour que le parquet accepte de lancer une commission rogatoire internationale. Or, il est toujours difficile de chiffrer les dégâts en matière d'Internet : s'il n'y a pas eu suppression ou vol de données, nous aurons du mal à obtenir une poursuite de l'enquête.

sur le Web ? *"Une chose est sûre : il n'y a pas de travail possible sans conservation des données,* justifie Christian Aghroum. *Entre le moment où l'on est saisi d'une enquête et le moment où l'infraction a commencé, il peut s'être écoulé plusieurs mois."* Sans compter que dans de nombreuses affaires, les pirates opèrent depuis l'étranger. Dans ce cas, une fois la provenance identifiée, il faut demander une commission rogatoire internationale, attendre que la police locale rassemble les éléments ou envoyer des enquêteurs sur place. Le système est lent alors que les criminels, eux, sont extrêmement réactifs et de plus en plus prudents. Ils déplacent les serveurs qui abritent des botnets (ces robots qui prennent le contrôle d'ordinateurs, *voir page 48*), multiplient les serveurs rebonds pour brouiller les pistes. *"C'est le problème de la lutte contre la cybercriminalité. Nous sommes encore sur une logique nationale alors qu'Internet est un phénomène extraterritorial. Il faudrait créer une Onu de la cybercriminalité"*, se prend à rêver Christian Aghroum.

Le plan de lutte présenté par la ministre de l'Intérieur prévoit le renforcement de la coopération internationale. Reste que dans ce domaine, les avancées sont parfois difficiles. Tous les pays ne sont pas au même niveau de compétence, n'ont pas le même niveau de législation. Parfois, c'est la volonté qui manque : certains, comme la Russie, sont ainsi devenus en quelques années de véritables paradis pour cybercriminels. • **N.Re.**

A DÉCOUVRIR !

CHEZ VOTRE MARCHAND DE JOURNAUX

Les pédophiles pris

Armés de technos et d'intuition, les gendarmes de Rosny arpentent le côté sombre du Web. *Dans leur collimateur : les pédophiles. Chats, peer-to-peer, mots-clés, ils font feu de tout bois pour piéger les cybercriminels.*

Rien de tel qu'un bel après-midi de printemps chez les gendarmes du fort de Rosny-sous-Bois pour repartir avec les idées noires ! Non pas qu'ils soient de mauvaise compagnie, au contraire, c'est plutôt la faute à leurs fréquentations… de travail. Des adresses IP qui font froid dans le dos et qui sont scannées tout au long de la journée, à la recherche d'un cybercrime bien particulier : la diffusion de contenus pédopornographiques. A priori, on n'a pas envie de se plonger dans cet univers glauque. Jusqu'à ce que l'on en mesure l'enjeu. Et que l'on devienne un peu plus parano qu'on ne l'était !

Première halte au département de surveillance de l'Internet – et plus spécialement des "chats, forums, IRC" – du service technique de recherches judiciaires et de documentation. Ici, les enquêteurs se forment au langage des plus jeunes, se connectent sur les salons de discussion, scrutent les réseaux où s'échangent des milliers de conversations en direct, et poussent les portes des IRC les plus privés. Car dorénavant, depuis la loi sur la délinquance votée en mars 2007, les investigations effectuées sous pseudonyme par des services habilités– la gendarmerie en fait évidemment partie– peuvent servir de preuve dans le cadre d'une enquête.

Les enquêteurs nous proposent une démonstration… On se connecte sur Voilà, dans un salon où se retrouvent les moins de 18 ans d'Île-de-France, et on se fait passer pour un garçon de 12 ans. À peine deux minutes plus tard, on reçoit une drôle d'invitation. L'internaute se présente comme un type de 19 ans et propose, au bout de deux échanges succincts, qu'on branche notre webcam. On répond qu'on n'en a pas, que maman n'est pas d'accord pour avoir une webcam à la maison. L'internaute insiste : *"Tu sais pas ce que tu rates."* Et là, ça dérape. Très vite, très mal. D'un seul coup, on voudrait jeter toutes les webcams aux orties. Pourtant, le chef d'escadron Alain Permingeat se garde bien de prodiguer des conseils, encore plus de faire la leçon. Il préfère éveiller les consciences en nous montrant son travail. Et agir. Car son objectif va au-delà de la lutte contre la diffusion de contenus pédopornographiques. Ce qu'il cherche, c'est faire tomber des pédophiles.

● UNE POIGNÉE DE GENDARMES TRAQUENT LES INFRACTIONS PÉDOPHILES SUR LES RÉSEAUX, au sein de la division "cyber-criminalité" du service technique de recherches judiciaires et de documentation de la gendarmerie.

Il sait que 80 % des pédophiles passant à l'acte sont d'importants collectionneurs d'images et de vidéos transgressives. Les cyberenquêtes sont donc devenues un moyen de traque. Alain Permingeat se souvient : *"L'affaire remonte à la fin août 2006. Tout est parti de la diffusion d'une image pédopornographique par un internaute de 28 ans. Finalement, ce sont 9 000 images que l'on a retrouvées chez lui. Et lors de sa garde à vue, il a reconnu avoir agressé sexuellement et violé sa sœur lorsqu'elle était mineure."* Les "N-Techs" (techniciens en nouvelles technologies) de ce service de gendarmerie poursuivent l'enquête sur le terrain, jusqu'à l'identification nominative de la personne cachée derrière le PC, la perquisition informatique… Tout démarre sur les réseaux peer-to-peer où ils pratiquent une surveillance proactive : ils n'attendent pas une plainte pour enquêter, mais vont débusquer eux-mêmes les infractions. S'ils connaissent bien ce que l'on nomme le "Web caché", les arcanes de la Toile, ils n'ont pas besoin d'aller aussi loin pour trouver une adresse IP. Ils fouillent tout ce qu'ils trouvent via des logiciels aussi connus que eMule, Kazaa, Direct Connect…

Un logiciel supersophistiqué

Devant nous, un gendarme tape le mot-clé "preteen" (préadolescent, en anglais) et repère en un clic le nombre de serveurs proposant des images ou des vidéos, le nombre de personnes connectées à ces serveurs, la quantité de fichiers qui s'y échangent et la localisation des serveurs. Comme il a l'embarras du choix, il sélectionne l'un d'eux au hasard parmi ceux hébergés en France. Ce jeudi-là, à 17 h, sur un serveur français connecté sur un réseau P2P et répondant à une recherche particulière sur un seul mot-clé… on découvre 1 100 fichiers en train de s'échanger

PHOTOS : PC GENDARME PHILIPPE LATRUBESSE - DR

dans la Toile

et 709 diffuseurs ! Plus ou moins à l'intuition, le gendarme arrête son curseur sur un diffuseur, enregistre son adresse IP, l'heure et la date de connexion, des informations qu'il transmettra au fournisseur d'accès Internet pour identifier l'abonné. Avant, il note les signatures électroniques des fichiers diffusés pour les comparer à une base de données maison.

Destination le Cnaip, Centre national d'analyse des images pédopornographiques, situé dans le même bâtiment, quelques bureaux plus loin. L'outil de travail : une base constituée de 500 000 images qui sert à la reconnaissance automatique de photos. *"Ça permet d'accélérer les recherches. On n'est plus obligé d'ouvrir les fichiers un à un"*, explique le responsable du centre. Une automatisation devenue indispensable quand on sait que les enquêteurs trouvent une centaine de fichiers pour un diffuseur rien qu'à partir d'un seul mot-clé, et dénichent jusqu'à une ou deux centaines de milliers de fichiers lors de la perquisition d'un gros diffuseur. Le logiciel du Cnaip effectue des rapprochements à partir des couleurs et des formes des photos. Il est capable de lier entre elles plusieurs victimes, ou des éléments de décor. Et ainsi, peut-être, d'aider les enquêteurs à confondre des suspects en identifiant leur lieu de vie. Lors de notre visite, sur une photo, un jeune garçon posait debout devant un mur bleu sur lequel on apercevait le coin de deux tableaux, dont on devinait que l'un représentait une baleine. En passant cette photo à l'épreuve de la base, et en zoomant sur une partie du mur et du tableau, plusieurs dizaines d'autres photos sont sorties. Avec le même fond bleu, les mêmes tableaux. Mais d'autres enfants, dans d'autres positions. • **D.S.**

LE CHIFFRE

Un gros diffuseur stocke sur son disque dur jusqu'à 200 000 fichiers à caractère pédopornographique.

TROUVER DES PREUVES ? FACILE !

Au fort de Rosny se trouve aussi l'Institut de recherche criminelle de la gendarmerie nationale : les pros de la preuve, de la "criminalistique". Une petite quinzaine de personnes traitent tous les supports informatiques et électroniques, localisent les appels GSM, interceptent les conversations du Net, récupèrent les données effacées, lisent les DVD rayés, les clés USB cassées, décodent des mots de passe, des dialogues codés. *"Dans la pédophilie, l'avantage avec les collectionneurs, c'est qu'ils gardent tout ! Mais même s'ils voulaient tout effacer, ils n'y arriveraient pas : on laisse des traces partout sur nos appareils numériques qui font tout à la fois"*, précise le capitaine Guillaume Duprez. Les téléphones, par exemple, prennent des photos, vidéos, gardent des SMS en mémoire... Le pendant, c'est que ça facilite le "happy slapping" (la diffusion sauvage de contenus violents ou pornos sur le Web). Au final, le plus dur, ce n'est donc plus de trouver une preuve, mais de faire le tri. *"Si l'on imprimait le contenu d'un disque dur de 250 Go, ça donnerait une pile de papier de 6 km de haut !"*, ironise le capitaine. Imaginez quand ils font 1 téraoctet...

©RGBDIGITAL_CO.UK - FOTOLIA.COM

Sur les lieux du crime,

Indices, traces, pièces à conviction... *Alexis Rimbaud, expert judiciaire nous dévoile son métier appliqué à la cybercriminalité.* ▪ **Propos recueillis par Delphine Sabattier.**

témoignage

Alexis Rimbaud a choisi le terrain : sa passion pour les nouvelles technologies, il l'a mise au service de la sécurité et de la justice. Il est ce qu'on appelle un "expert" et intervient dans le cadre pénal d'affaires de crime et de terrorisme. Un métier dangereux, qui n'a pas d'horaires. Une vocation parfois mise à rude épreuve. Lorsque nous l'avons rencontré, il hésitait vraiment à parler de tout ça. Surtout pas envie de se donner en spectacle. Peur que l'on se méprenne sur son travail, aux contours complexes. L'expert Alexis Rimbaud que nous avons découvert au fil de notre entretien est exigeant avec lui-même, à la mesure des résultats qu'on attend de lui. Les informations qu'il rassemble peuvent faire basculer du jour au lendemain toute une enquête policière ou renverser l'opinion d'un juge. Un métier à haute responsabilité qui a attisé notre curiosité. Nous lui avons donc ouvert ces pages afin qu'il nous plonge, avec ses mots et à travers ses histoires vraies, dans l'univers de l'expert pénal spécialiste en cybercriminalité.

Un travail solitaire et exposé

L'image des *Experts* véhiculée par la télévision est assez éloignée du quotidien de l'expert judiciaire spécialiste en cybercriminalité. Qu'il habite Manhattan, Miami ou Garges-lès-Gonesse, sa tâche répond autant aux normes imposées par le cadre légal qu'à celles de la maîtrise des technologies scientifiques d'investigation les plus avancées. Les exploitations effectuées par l'expert indépendant national, comme celui au service du FBI, n'échappent pas à la règle. Loin du glamour, la gestion administrative de son travail peut occuper jusqu'à 60 % de son temps. Il n'est pas un représentant de l'ordre, mais juste un auxiliaire de justice. L'expert judiciaire est par ailleurs un homme seul. Cette indépendance a un coût. Il engage sa responsabilité devant les tribunaux et le fait de façon personnelle, moralement et physiquement en se confrontant au contradictoire, par écrit ou en se présentant aux juges lors du procès. Il ne bénéficie d'aucune protection particulière, utilise son propre matériel, souvent ses propres deniers, ses propres logiciels commerciaux ou non, et n'est lié ni à l'institution judiciaire, ni à un service.

> *L'expert ne bénéficie d'aucune protection, utilise son propre matériel, ses propres logiciels et souvent ses propres deniers*

Lors d'une ordonnance dont j'ai eu la charge, il y a quelques années, ma mission consista à assister des policiers ainsi qu'un magistrat instructeur durant une perquisition au sein d'une grande entreprise française. À l'aube, je traversai Paris et la grande couronne embrumée, sur mon scooter équipé des trois valises de matériel d'analyse. Cette opération de police faisait suite au dépôt de plainte d'un internaute pour *'intrusion suivie de destruction...'* puis, pour l'utilisation frauduleuse de son compte mail. Les officiers de police judiciaire avaient établi, lors de leur enquête préliminaire, que l'adresse IP utilisée pour l'infraction était celle de cette entreprise. Notre arrivée dans les locaux flambant neufs se passa dans les meilleures conditions. À mon niveau, la simple identification d'une adresse IP est loin d'établir un lien réel entre les protagonistes de ce genre d'affaire, mais ma mission était de *'faire apparaître tout élément en rapport avec des tentatives d'intrusion sur la machine de M. X, toute manipulation visant à effectuer ce genre d'infraction, toute trace faisant état d'un lien entre l'entreprise Y et M. X'*.

Dans son bureau, le sympathique et bedonnant directeur de la sécurité informatique (DSI), dont la formation d'expert comptable n'allait pas être d'un grand recours, ignorait visiblement les responsabilités de sa charge.

L'entreprise était constituée d'un réseau de plus de 200 postes gérés par un serveur ayant pour tâche non seulement le firewalling (pare-feu, *ndlr*), mais aussi la gestion des mails au travers d'un serveur Microsoft Exchange, ainsi que le partage des données selon des droits établis au jour le jour et les exigences de l'instant...

Comment effectuer des dizaines de copies de disques durs, sur des serveurs en fonctionnement qui plus est ? A priori, il pouvait s'agir de n'importe quel poste informatique de l'entreprise, mais à ce moment précis, devant le peu de réaction du

PHOTOS : © POINT TRAIT

place à l'expert

DSI depuis longtemps dépassé, je décidai de comparer l'adresse IP fournie en procédure identifiée comme celle de l'entreprise à celle affichée par les serveurs devant nous. Elles ne correspondaient pas. Surpris, j'en faisais état au magistrat qui questionna le dirigeant de l'entreprise. En réalité, cette adresse IP était celle d'un réseau secondaire Wi-Fi, destiné à certains visiteurs de passage. Mais à la date des faits, nous ne trouvions personne dans cette enceinte, protégée par un code d'accès.

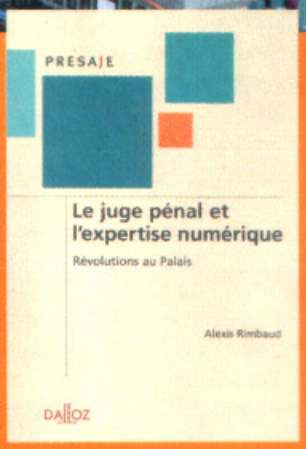
En compagnie du DSI, j'auscultai la salle des "invités". Elle était équipée d'une petite borne peu puissante et réservée à des situations rares. L'utilisation d'un analyseur de fréquences permit d'établir que le signal ne dépassait pas la pièce. En revanche, cette salle donnait sur une cour fermée. Dans le même temps, je récupérai les traces de connexions (logs) du petit boîtier Wi-Fi, ainsi que sa clé Wep. Me penchant à la fenêtre dans la cour, je distinguai assez clairement une petite

ALEXIS RIMBAUD, auteur de terrain

Alexis Rimbaud est spécialiste des nouvelles technologies de l'information et consultant en systèmes d'information. Il a été maître-assistant à l'université Paris VIII. Fort d'une expérience de plus de 15 ans en entreprise et au service de la justice, il dirige un groupe pédagogique visant à sensibiliser les dirigeants d'entreprises aux imbrications entre technologie et obligations légales. Fort de son expérience au service de la justice, il a écrit *Le juge pénal et l'expertise numérique*, un livre référence qui mêle déontologie, contraintes de terrain, technologies de pointe et procédure pénale. Cet ouvrage se décline autour de trois idées découlant de l'usage des nouvelles technologies en matière pénale :

- l'identification de tout individu est possible partout et à chaque instant par l'analyse des traces qu'il laisse derrière lui sur les réseaux et les machines ;
- l'accès aux informations tirées de l'infiniment petit, ouvre de nouvelles pistes pour élucider les crimes de sang ;
- la traque des circuits de la criminalité financière s'affranchit des contraintes de temps, d'espace ou de droits locaux.

Le juge pénal et l'expertise numérique **est coédité par Presaje et Dalloz. Disponible en librairie, format 240 x 160, 200 pages, 25 €.**



● L'ANALYSE DE DISQUES DURS VOLONTAIREMENT DÉTRUITS (par balle sur notre photo) réclame, lorsqu'elle est possible, des connaissances et des outils très spécifiques.

antenne Wi-Fi placée au dernier étage de l'immeuble d'en face. Une petite antenne amplifiée de 8 dBi dirigée vers nous. L'examen de l'ordinateur du locataire indélicat permit de reconstituer la clé Wep de l'entreprise, ainsi que plusieurs outils destinés à l'intrusion.

Une dose d'intuition

Si la maîtrise des systèmes d'information permet une vue scientifique des situations, c'est le respect des règles de droit et souvent le recul qui permettent de comprendre les mécanismes d'intrusion.

Dans une autre affaire, une jeune femme de 17 ans portait plainte pour viol contre un homme de 62 ans rencontré sur l'Internet. L'homme avait reconnu les échanges avec la jeune femme au travers de l'Internet, mais pas l'intégralité des faits.

Le juge d'instruction me confia la mission de reconstituer les éléments de leurs échanges sur la machine du mis en cause, placée sous scellé judiciaire, et d'établir l'intégralité des contacts et activités de cet homme. Or, il m'apparaissait intéressant de suggérer au magistrat de figer rapidement les éléments des deux parties, non seulement la machine du mis en examen mais aussi celle de la victime, ceci, afin de reconstituer méthodologiquement la cohérence absolue des faits. Le magistrat ordonna le placement sous scellé de la machine de la victime et je me rendis chez elle afin que ses parents nous confient l'ordinateur.

Concernant cette machine, les premiers éléments expertisés permettaient de déterminer qu'elle possédait effectivement une connexion Internet, mais l'analyse poussée de sa machine permit aussi d'établir que deux heures après avoir porté plainte, la jeune femme avait totalement reformaté son disque dur, ayant pris soin de ne sauvegarder que les éléments relatifs à l'affaire en cours. La reconstitution des parties formatées de son disque dur permit de mettre au jour le profil d'une adolescente passant 4 à 6 heures par jour sur les sites de rencontre, tenant des propos sans équivoque sur les buts de ses contacts. À grand renfort de photographies et de descriptifs détaillés, elle proposait ses charmes à une cinquantaine d'hommes, tous

âgés de plus de soixante ans, se décrivant comme une étudiante de 20 ans, esseulée et déçue par la jeune génération. Surprise par ses parents lors d'un échange avec l'homme, la jeune femme tenta de se justifier en l'accusant en retour. Les parents prirent le relais en l'accompagnant lors de la plainte.

Self-control et rigueur sans faille

La survenance d'événements accidentels, de faits délictueux ou l'arrivée sur le lieu d'un crime sont des situations qui réclament de la part de tout expert, y compris en informatique, un self-control absolu, même face aux scènes les plus violentes. L'expert pénal intervient sur mission d'un magistrat instructeur, sur réquisition d'un officier de police judiciaire ou du parquet, ou enfin sur demande d'une juridiction de jugement qui lui confie une mission parfaitement cadrée. Des normes définissent les méthodes de travail, les outils pouvant être utilisés, et imposent une reproductibilité des constatations et conclusions, sous peine d'invalidité de l'expertise, voire de sanctions envers l'expert. Ainsi, la lutte contre la cybercriminalité ne peut-elle être menée efficacement qu'à la condition absolue d'une maîtrise des outils mis à notre disposition par les codes de procédure civil, commercial et pénal. À cela s'ajoute, bien sûr, une connaissance aiguë et constante des techniques scientifiques stabilisées. C'est à ce prix que l'expert peut mettre son savoir à la disposition de la justice et défendre son travail qui, loin des sphères de pouvoir et de certains clichés, vise à l'établissement de la vérité.

LES OUTILS DE L'EXPERT

Il n'existe pas d'outils véritablement adaptés à l'intégralité des cas de figures et il est généralement plus efficace de développer ses propres produits, matériels ou logiciels.
Toutefois, parmi les outils de base de l'expertise, nous trouvons l'utilisation de boîtiers permettant la lecture "off line" des données des disques durs. Ces blocs de lecture diffèrent des boîtiers externes classiques par le fait qu'ils interdisent toute écriture sur les disques examinés. Ces systèmes "expertaux" – du type "fast block" ou plus sophistiqués, tel Forensic Phantom de Logicube – permettent l'exploitation ou la copie des disques dans le respect des conditions judiciaires : ils génèrent des images-disques pouvant supporter l'exploitation en l'absence du support original. L'image du disque générée doit être "hashée", c'est-à-dire qu'un "code empreinte" est généré par un algorithme identifiant de façon unique le disque original. Concernant les événements réseaux, nous pouvons évoquer de nombreux logiciels comme Wireshark ou TCPDump. La liste est longue, mais les objets analysés par l'expert sont polymorphes et le champ des connaissances est vaste : analyse des mails détruits sur un serveur d'entreprise, reconstitution de disques intentionnellement détruits (par l'acide ou autres procédés), téléphonie et toutes ses applications embarquées, ou encore classification hiérarchique du rôle d'un individu au sein d'un réseau pédophile.
Dans certains cas, nous devons analyser les flux satellites reçus par des GPS afin d'en valider la valeur lors d'un accident de la route. Dans d'autres, il s'agit de connaître l'intégralité des fréquences émises dans un périmètre donné. Il arrive enfin, que certaines affaires nécessitent une adaptation en temps réel de nos outils. C'est en particulier le cas pour les extorsions de fonds ou les enlèvements, lorsque le temps est un facteur important. Nous devons alors mettre au point des outils in situ. La programmation de petits logiciels en C (ou pour ma part, en Pascal/Delphi) est souvent la solution. L'usage du fer à souder n'est pas chose rare, et la fabrication de modules électroniques durant la survenance des faits est parfois nécessaire.

La "trousse" d'Alexis Rimbaud est un capharnaüm d'outils aussi variés que les situations qu'il rencontre. Elle se complète d'une vaste panoplie de logiciels, qu'il programme souvent lui-même.

Logiciels de sécurité : ju

De l'art de bien se prémunir. *Armé jusqu'aux dents, votre PC a bien sûr plus de chances de sortir indemne de vos pérégrinations. Mais ne comptez pas sur une immunité totale !* • par D.S et J.H.

à nouvelles menaces, nouvelle stratégie. Hier, les virus et les vers qui se transmettent via le réseau et non par le biais d'un support physique comme les virus dominaient. Aujourd'hui, les menaces se sont modifiées et diversifiées, obligeant les éditeurs de solutions de sécurité à multiplier les parades. C'est certain qu'avec une bonne pratique du mail et de l'Internet, en respectant les principes de sécurité élémentaires (ne pas ouvrir n'importe quelle pièce jointe, bien choisir ses mots de passe et ne pas les divulguer, ne pas s'aventurer sur des sites à risque, etc.), on sera plus à l'abri qu'un autre… et encore, à condition de ne pas en être trop certain ! Soyons clair, dès lors qu'on utilise son ordinateur fréquemment, on court un risque.

Derrière le terme virus, les spécialistes regroupent maintenant plusieurs menaces. Les virus sont devenus plus généralement des programmes malveillants (malwares): chevaux de Troie, keyloggers, spywares… Un moment d'inattention et vos données privées se retrouvent kidnappées. Par qui ? Selon François Paget, secrétaire général du Clusif (Club de la sécurité de l'information français) et chercheur chez l'éditeur McAfee, 80 % des attaques visent le monde financier ou bancaire. Avec vos mot de passe et identifiant, les pirates peuvent vider vos comptes en un temps record. Les jeux en ligne sont aussi devenus une cible intéressante pour les malfaiteurs, concernant 15 à 20 % des chevaux de Troie, toujours selon le Clusif. Ils subtilisent des comptes d'utilisateurs et revendent des pouvoirs virtuels contre argent comptant. Sur les sites d'e-commerce, ils interceptent les paiements… Que peut un antivirus contre ces attaques ? Tout seul, pas grand-chose ; l'idéal, disent les spécialistes, est de s'assurer un maximum de protections spécifiques et donc de se tourner vers les suites logicielles complètes (*voir ci-dessous*).

Ainsi, votre antivirus pourra se reposer sur un filtre antiphishing, par exemple, qui saura reconnaître un message suspicieux dans votre boîte mail (c'est généralement comme ça que commence une opération de phishing) et une adresse mail falsifiée. Car lorsqu'une attaque de phishing est détectée, les adresses IP des faux sites sont collectées et inscrites dans une base. Tout le problème, c'est qu'il s'agit d'une protection a posteriori, l'outil ne pouvant pas deviner à l'avance les sites qui seront créés par les malfrats… Des difficultés comme celles-là, et bien d'autres, tous les outils de sécurité, même les plus professionnels, en rencontrent.

Un internaute averti en vaut deux. Nous vous invitons ici à un petit tour d'horizon des principales menaces et des parades disponibles.

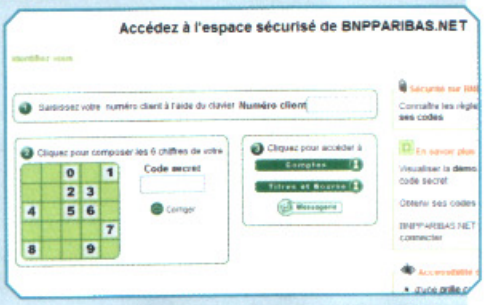
LES SUITES DE SÉCURITÉ FONT PEAU NEUVE

Leur travail, c'est de tout faire, du sol au plafond. Antispyware, antivirus, protection contre les vers du Net, prévention d'intrusion, authentification de sites Web, protection contre l'espionnage, gestion des informations confidentielles… les suites complètes représentent une solution idéale pour se sentir correctement protégé. Bonne nouvelle, qui plus est, les durées d'abonnement aux mises à jour s'allongent à deux ans pour certaines et les éditeurs ont pris en compte l'importance du multi-équipement chez les

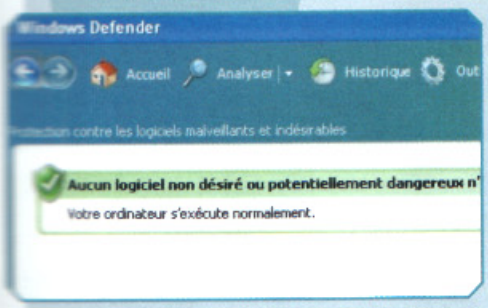
squ'où protègent-ils ?

Spyware, vol à l'arraché

Les spywares (espiogiciels ou logiciels espions en français) cherchent à récupérer des informations confidentielles à l'insu de l'utilisateur. Ces spywares peuvent être incorporés à certains freewares malveillants ou être indépendants. Il en existe de différentes sortes. Les spywares classiques analysent le contenu des disques durs et peuvent extraire des données depuis les zones dites sécurisées de Windows. Les enregistreurs de frappe clavier (keyloggers) s'attachent pour leur part à capturer à la volée les identifiants et mots de passe. D'autres, les enregistreurs vidéo, capturent les actions à l'écran, certains services bancaires ayant remplacé la frappe clavier du mot de passe par des clics souris sur un clavier virtuel. Un bon moyen de bloquer ces attaques est d'utiliser un navigateur virtuel, rendant les captures d'écran impossibles (à la manière des alertes UAC de Vista, qui exploitent aussi la virtualisation). Mais on peut aussi virtualiser le clavier pour contrer un keylogger.



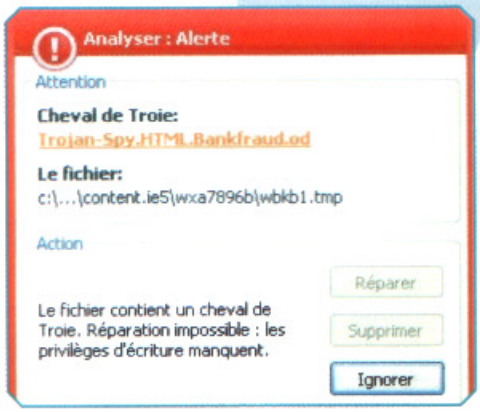
Un clavier virtuel permet aux clients de la BNP de saisir leurs détails bancaires sans crainte qu'ils soient interceptés par un keylogger.



Windows Defender est un antispyware intégré à Windows Vista, et facile à ajouter sur Windows XP.

Cheval de Troie en éclaireur

Bien que non contagieux (le programme doit être exécuté par l'utilisateur par chargement d'une pièce jointe ou d'un programme censé être utile), le cheval de Troie n'en est pas moins redoutable. Sa fonction première est d'introduire une porte dérobée (backdoor) compromettant la sécurité du système. Ensuite, le pirate pourra à loisir explorer le contenu des disques durs, installer de nouveaux malwares et dans la plupart des cas prendre le contrôle à distance du poste pour en faire un ordinateur zombie au sein d'un botnet : groupés par milliers voire dizaines de milliers, ces ordinateurs zombies peuvent être exploités par le pirate (ou la pègre à qui le pirate a revendu le réseau de bots), à l'insu de leurs propriétaires, pour mener des actions de grande envergure : attaque DDOS (déni de service distribué) pour bloquer des serveurs (avec demande de rançon), envoi massif de spams ou phishing. Ces programmes sont détectés par les antivirus, mais leur nettoyage peut réclamer une réinstallation du système.



La détection d'un cheval de troie est à la portée d'un antivirus. Son éradication, en revanche, peut être plus problématique.

Pharming, en route pour l'abattoir !

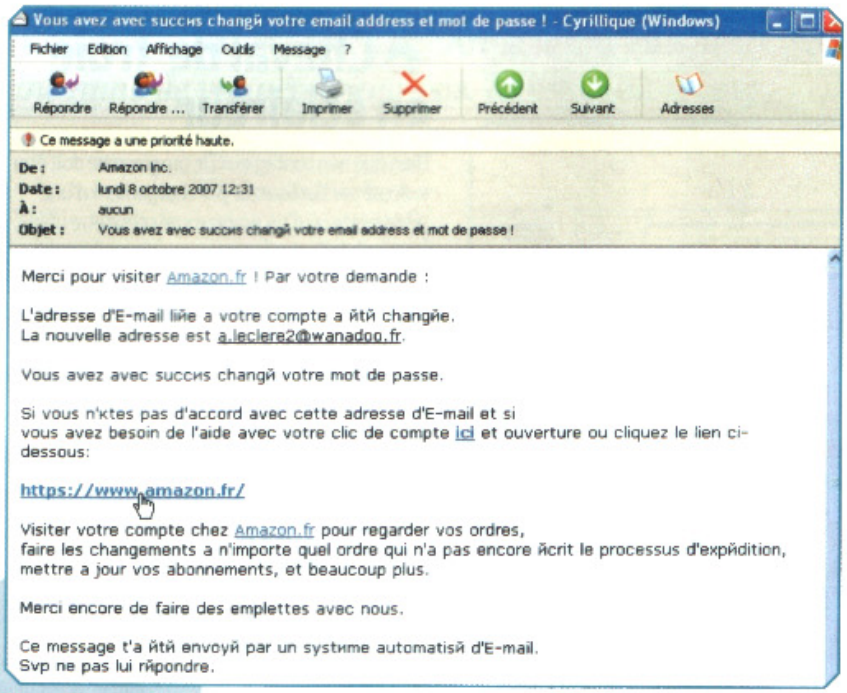
Proche du phishing dans son principe (tromper l'internaute et le conduire sur un site différent du site prévu), le pharming, en pleine expansion, est redoutablement efficace. Il s'attaque directement aux serveurs DNS non sécurisés (les serveurs qui convertissent l'adresse Web en adresse IP). L'utilisateur, qui accède normalement à un site connu ou clique sur une entrée des résultats d'un moteur de recherche, se retrouve à son insu redirigé vers un autre site. Une variante du pharming est l'injection d'un code Javascript de redirection dans des serveurs Web piratés. Le site de destination est un véritable laboratoire pirate, contenant un cocktail explosif de logiciels malveillants cherchant à exploiter des vulnérabilités de Windows ou de logiciels tiers (RealPlayer, Safari, lecteur Flash Adobe, etc.) pour installer spywares et autres chevaux de Troie. Ces attaques sont de plus en plus massives et peuvent toucher plusieurs centaines de milliers de serveurs Web simultanément.

particuliers. Quasiment tous autorisent l'installation sur plusieurs machines (jusqu'à trois) de leurs produits, sans surcoût. Elles fonctionnent bien entendu indifféremment sous XP ou Vista.

Norton 360 version 2.0, la nouvelle version de la suite de sécurité grand public de Symantec est désormais disponible. Toujours aussi facile à utiliser pour les novices, elle offre désormais aux habitués des paramétrages et un usage avancés. Elle assure une protection contre tous types de menaces : spywares, virus, vers Internet, contrôle d'accès, rootkits, prévention d'intrusion, protection contre l'espionnage, etc., la détection profitant de l'analyse comportementale. Elle vérifie aussi la sécurité du réseau (filaire et sans-fil), offre un outil pour gérer mots de passe et formulaires et fournit un diagnostic détaillé de la configuration. Elle gère aussi la sauvegarde off et online, sur un espace réservé de 4 Go. L'installation est possible sur trois machines. Prix : 90 €, avec 1 an de mises à jour garanties.

Kaspersky, avec sa version 8, tout juste sortie sous le nom d'Internet Security 2009, inaugure une nouvelle génération de logiciels de protection. La suite intègre un système de restriction des privilèges d'accès des programmes aux ressources du système. De cette manière, les malwares ne pourront plus exécuter leurs actions malfaisantes. Cette défense s'ajoute à la détection des malwares par signature (la réactivité contre les nouvelles menaces a été encore augmentée) et à l'analyse comportementale. Cette version profite encore de la recherche/suppression des vulnérabilités détectées dans le système d'exploitation comme dans les applications, d'un clavier virtuel (pour parer aux keyloggers) complété d'un blocage des tentatives de vol des données échangées sur les connexions sécurisées, d'une base enrichie de sites connus de phishing.

Phishing : ne mords pas à l'hameçon !

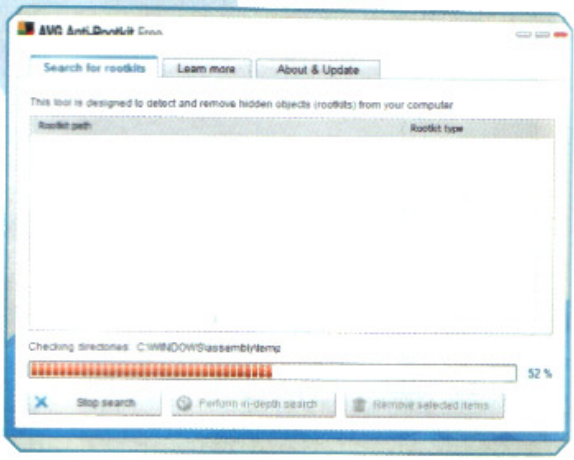


Attention, mail piégé ! Ici, un mail invite l'internaute à se rendre sur un faux site Amazon. Si le texte du mail paraît louche, car rédigé dans un français approximatif, il y a fort à parier que le site miroir d'Amazon sera, lui, très ressemblant.

Le phishing repose sur l'utilisation d'un site miroir (un faux site utilisé par les malfaiteurs pour piéger les internautes et les inviter à laisser leurs données confidentielles). Il repose aussi le plus souvent sur l'utilisation de plusieurs "PC zombies", des ordinateurs contaminés en vue d'organiser une attaque, en général à l'insu de leurs propriétaires. Ce qui permet éventuellement aux pirates de changer l'adresse IP du site miroir toutes les 5 minutes ! Autant dire que la manipulation devient corsée pour trouver – et interdire – toutes les machines impliquées dans l'attaque. Pour ne pas faire partie de la liste des zombies, la meilleure parade est d'utiliser une solution complète de sécurité combinant antivirus, pare-feu et tout ce qui est susceptible de repérer un programme malveillant s'installant sur votre ordinateur. L'antiphishing intègre souvent plusieurs technologies complémentaires. Le message spam initial sera reconnu directement ou suspecté en fonction du serveur d'envoi (liste tenue à jour en temps réel des serveurs d'envois massifs, domaine, pays). La liste noire des sites de phishing reconnus fournit une bonne protection : elle interdit l'accès à un tel site. Mais elle ne fonctionne qu'à partir du moment où l'attaque a déjà été répertoriée : les premières victimes d'un phishing ne seront donc pas protégées. Pour combler ce décalage, les outils de protection contre le phishing analysent aussi le code de la page Internet, à la recherche de procédures suspectes.

Rootkit, la tenue de camouflage

Les rootkit sont des programmes très particuliers, issus du monde Unix, dont l'objectif est de prendre contrôle d'une machine (plus précisément d'avoir l'accès "root", qui donne accès à toutes les fonctions et même au matériel) à l'insu de l'utilisateur. Dans l'univers des virus Windows, leur fonction est de cacher un autre malware déjà installé, en l'occurrence un cheval de Troie. C'est ce dernier qui compromet effectivement la sécurité du poste. Mais le rootkit le rend très difficile à détecter en masquant son processus Windows, des fichiers ou des clés de registre. Les antivirus sont capables de supprimer bien des rootkits, mais d'autres échappent à leur surveillance et obligent à utiliser un produit spécifique, un "antirootkit". *"L'antirootkit touche aux niveaux les plus profonds du système, c'est une usine à gaz qu'on active à la demande. Une fois par semaine est un bon rythme pour une navigation Internet soutenue"* indique François Paget, secrétaire général du Clusif. En lançant Vista, dont le noyau est bien mieux protégé que celui de XP, Microsoft s'était vanté d'en avoir fini avec les rootkits. Ils sont effectivement moins nombreux sous le nouvel OS, mais existent tout de même bel et bien !



Un antirootkit, intégré par exemple à une suite de sécurité, agit au niveau le plus profond du système et est activé à la demande.

● ● ● de l'analyse des connexions Wi-Fi et de diverses améliorations complémentaires (interface, assistants, antispam, contrôle parental...). Prix : 70 € pour une licence d'un an valable pour trois postes.

ET AUSSI...
G-Data TotalCare 2008, McAfee Total Protection 2008, Norman Security Suite 2008, Panda Internet Security 2008, BitDefender Total Security 2008, F-Secure Internet Security 2008
Ces suites de sécurité peuvent être renforcées par un outil complémentaire, ZoneAlarm ForceField de CheckPoint, annoncé depuis de longs mois et enfin disponible. Cet outil offre une sécurisation accrue du navigateur, point d'entrée désormais privilégié des attaques. Le principe consiste à virtualiser le navigateur. Toutes les modifications initiées depuis le navigateur (exploitation de vulnérabilités, téléchargement Web automatique, spywares, virus, etc.) sont effectuées sur le système de fichiers virtuel, qui disparait à l'arrêt du surf. Cette virtualisation est complétée d'une protection complémentaire antiphishing (signatures + heuristique), d'un brouilleur d'enregistreurs de frappe et de défenses additionnelles. Prix : 19,50 € pour un poste, 32,50 € pour trois postes.

Enfin, si vous privilégiez les solutions gratuites, il faudra faire votre shopping de-ci, de-là. Pour un antivirus, vous pouvez vous tourner vers Avast, AVG, Antivir Personal Edition ou F-Prot. Pour les pare-feux, vous avez le choix entre ZoneAlarm, Comodo, Outpost, Jetico (*voir page 56*) ou Sunbelt (alias Kerio). Enfin, côté antispyware-antiadware, vous pouvez exploiter Ad-Aware, Spybot Search & Destroy ou Windows Defender (celui de Microsoft, *voir page 58*).

Think
Smart Security*
ESET
Smart
Security
La nouvelle protection
intelligente pour votre PC
E-mails, messageries instantanées, téléchargements, achats en ligne, opérations bancaires... exposent constamment votre système et vos précieuses données aux multiples dangers véhiculés par Internet.
Il existe de nombreuses solutions logicielles de sécurité, mais l'une d'entre elles est différente : ESET Smart Security.
Fondée sur la technologie ThreatSense® maintes fois primée, la solution tout-en-un ESET Smart Security, en anticipant les dangers potentiels, protège de manière proactive votre ordinateur sans le ralentir.
L'alliance de 4 modules pour une protection intégrale :
ESET NOD 32 ANTIVIRUS
ESET NOD 32 ANTISPYWARE
ESET PERSONAL FIREWALL
ESET ANTISPAM
Contactez-nous par téléphone au 01 55 89 08 85 ou évaluez gratuitement ESET Smart Security pendant 30 jours, en téléchargeant la version d'essai depuis notre site :
www.eset-nod32.fr
NOD32 élu Antivirus de l'année en 2006 et 2007
NOD32 : record de récompenses aux tests Virus Bulletin
NOD32
AV comparatives
vb 100 VIRUS
49 récompenses VB100%
we protect your digital worlds**
eset
* Pensez à la sécurité intelligente ** nous protégeons votre monde numérique

Pour/Contre : doit-on com

En avoir ou pas. *Pour les éditeurs d'antivirus, pas de doute : sans antivirus, vous êtes mort ou ça ne va pas tarder, et ils se font forts de vous protéger quoi qu'il arrive. Mais ce n'est pas l'avis de tout le monde : des experts en sécurité jugent ce combat perdu d'avance, et qu'il vaut mieux tabler sur l'éducation du public. La parole à l'accusation et à la défense.* • **Propos recueillis par Nicolas Reynaud**

Éric Filiol

Il est directeur des laboratoires de cryptologie et de virologie de l'École supérieure informatique, électronique, automatique de Laval et de l'École supérieure et d'application des transmissions de Rennes.

SVM : Dans le livre que vous avez écrit sur la cybercriminalité (*éditions Dunod*) avec le journaliste Philippe Richard, vous parlez d'intox marketing à propos des antivirus. N'y allez-vous pas un peu fort ?

Éric Filiol : Quand les éditeurs marquent sur leur boîte ou leur site que leur solution détecte 100 % des virus, on est dans une démarche proche de l'escroquerie. Même s'il est impossible de donner un chiffre exact, on estime aujourd'hui qu'il y a entre 250 000 et 300 000 virus connus. Les antivirus sont loin de tous les détecter. Et quoique les éditeurs fassent ou disent, leur efficacité restera limitée. En 1986, Fred Cohen, un chercheur américain considéré comme le père de la virologie informatique, a démontré mathématiquement dans une thèse qui a fait date qu'il était impossible de faire un programme qui détecte systématiquement les virus. Depuis, de nombreuses recherches ont montré que beaucoup de virus rencontrés en pratique dans nos ordinateurs ne peuvent être repérés par les antivirus compte tenu de la complexité calculatoire du problème posé par leur détection.

> *« IL SUFFIT DE MODIFIER UN SEUL OCTET D'UNE SOUCHE CONNUE POUR LA RENDRE INDÉTECTABLE »*

SVM : Pourquoi ce décalage entre ce qui est annoncé et la protection effective ?

É.F. : Il faut comprendre que les solutions de sécurité ne peuvent détecter que les malwares qu'elles connaissent, qui sont répertoriés dans leur base de signatures. Selon les éditeurs, cette dernière est plus ou moins complète. Aucune marque ne peut se permettre de proposer un produit qui amoindrit les performances du PC. L'utilisateur risque de le désactiver ou d'aller voir du côté de la concurrence. Du coup, les bases sont allégées, les souches anciennes supprimées. Elles sont réinjectées seulement si elles ont un regain d'activité. Les éditeurs ont remplacé la richesse des bases par la fréquence des mises à jour. Certains éditeurs en proposent une centaine par semaine.

SVM : C'est une course sans fin...

É.F. : Tout à fait, et les pirates ont toujours une longueur d'avance. Il est très facile de contourner un antivirus. Dans l'absolu, il suffit de modifier un seul octet d'une souche connue pour qu'elle ne soit plus détectée. C'est à la portée de n'importe quel étudiant en première année d'informatique. L'autre problème, c'est que même quand ils sont capables de détecter un programme malveillant, les antivirus ont de plus en plus de mal à nettoyer l'ordinateur infecté. Certains malwares sont construits sur des technologies qui rendent la suppression quasi impossible. L'utilisateur n'a pas d'autre choix que de tout écraser et de tout réinstaller. Les éditeurs ne sont pas très diserts sur ce point.

SVM : Les éditeurs mettent en avant de nouvelles technologies capables de détecter des virus non connus,

Jean-Philippe Bichard est le porte-parole pour la France de la société russe Kaspersky, éditrice d'antivirus.

Jean-Philippe Bichard

pter sur les antivirus ?

grâce notamment à l'observation du comportement des fichiers...

É.F. : Le principe est le même que pour les bases de signatures. L'antivirus ne va détecter que les comportements dangereux qu'il connaît. En plus, ces systèmes sont, eux aussi, assez faciles à contourner. Les antivirus ne consacrent qu'un nombre limité de cycles machines à l'étude d'un fichier douteux. Il suffit de faire un virus qui va mettre 10 minutes pour agir. Personne n'est prêt à attendre autant de temps chaque fois qu'un fichier douteux se présente... La logique commerciale qui impose une fluidité aux antivirus n'est pas compatible avec une sécurité efficace. Il faut que les utilisateurs comprennent qu'instantanéité et sécurité ne peuvent pas aller ensemble.

SVM : Mais alors que peut-on faire pour protéger sa machine ?

É.F. : Je crois à l'éducation. En une génération, on obtiendra de bien meilleurs résultats qu'avec la multiplication des solutions techniques, et à moindre frais. Le principal intérêt des antivirus est de sensibiliser les utilisateurs à la sécurité. Cependant sans un minimum de précautions, cela ne sert pas à grand-chose. C'est comme quand vous conduisez. Ce n'est pas parce que vous avez le permis et une police d'assurance que vous n'aurez pas d'accident. Si vous avez une solution de sécurité et que vous ne mettez pas à jour votre système d'exploitation, que vous téléchargez des fichiers pirates, que vous allez sur des sites à risque, vous aurez toutes les chances que votre machine soit contaminée quelle que soit la solution de sécurité que vous utilisez. ●

SVM : Quel niveau de protection peut-on espérer en achetant un antivirus ?

Jean-Philippe Bichard : Les éditeurs sérieux recensent toutes les souches récentes ou en activité connues. Ils ont des équipes de chercheurs capables de développer de plus en plus vite des antidotes pour les malwares qui apparaissent. L'utilisateur peut compter sur un bon niveau de protection s'il choisit un éditeur qui dispose d'une véritable expertise, qui propose un service de mise à jour régulière de la base de signatures.

SVM : Des chercheurs dénoncent les limites de cette approche par comparaison et accusent les éditeurs de surévaluer l'efficacité réelle de leurs solutions...

J.-P. B. : 250 millions de personnes utilisent un antivirus. Je ne pense pas que tous ces gens se soient équipés d'une solution de sécurité si les produits que nous proposons n'étaient pas à la hauteur. Il y a des tests en laboratoire qui prouvent l'efficacité des antivirus quand les éditeurs assurent un vrai service derrière. D'où l'importance des mises à jour. Aujourd'hui, il s'agit plus de savoir si la protection se renforce ou devient plus superficielle compte tenu de l'apparition de nouvelles menaces, de la multiplication des codes malveillants.

SVM : Vous avez du mal à suivre ?

J.-P. B. : La cybercriminalité s'est professionnalisée. Il existe désormais un véritable marché du malware. Notre base de signatures à elle seule compte déjà 770 0000 souches ou codes malveillants. Les éditeurs ont conscience qu'ils ne pourront pas indéfiniment faire grossir les bases de signatures. Cela nous oblige à aller vers une approche plus comportementale, à développer des suites plus intelligentes, capables de détecter des virus que nous ne connaissons pas encore.

SVM : Sur quelles méthodes de détection s'appuient les suites de dernière génération ?

J.-P. B. : Nous faisons de la recherche pour essayer de passer de la réaction à la prévention. La plupart des virus peuvent être détectés par des méthodes semi-automatiques. 30 à 35 %, cependant, doivent être traités manuellement. Les nouvelles méthodes permettent d'identifier ces programmes malveillants encore inconnus du logiciel antivirus grâce à des algorithmes très sophistiqués. Le moteur analyse le comportement du fichier dans un sas et donne le choix à l'utilisateur en lui indiquant s'il est risqué ou non d'ouvrir le fichier.

> *« NOUS FAISONS DES RECHERCHES POUR ESSAYER DE PASSER DE LA RÉACTION À LA PRÉVENTION*

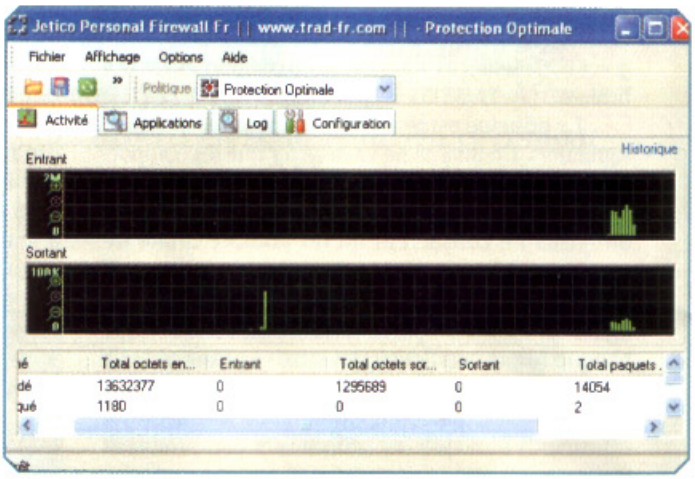
SVM : Ces nouvelles méthodes de détection ne risquent-elles pas de ralentir la machine ?

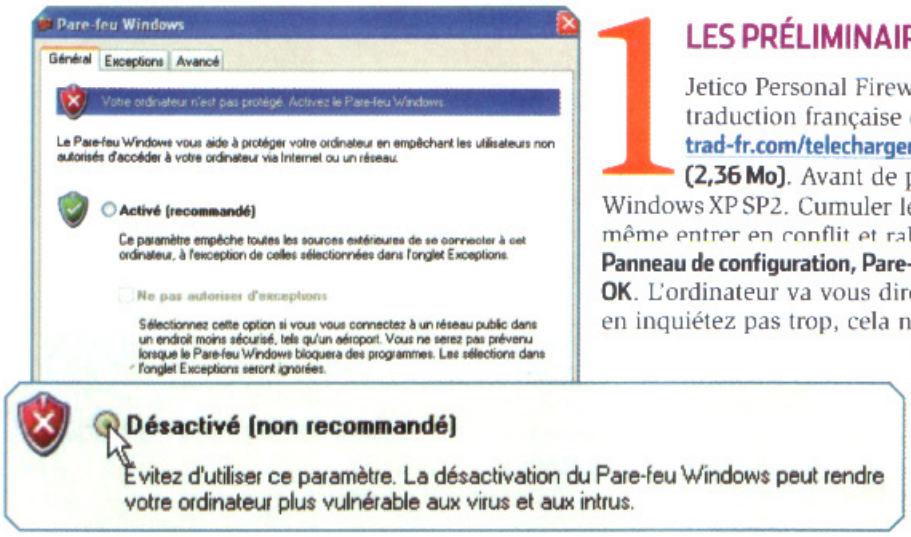
J.-P. B. : Les performances des ordinateurs d'aujourd'hui permettent une analyse rapide des fichiers. On peut faire un scan de disque dur en moins de 15 minutes. C'est l'adaptation de suites de sécurité aux smartphones qui risque de poser problème. Il va y avoir de plus en plus de virus pour ces terminaux qui sont beaucoup moins puissants que les ordinateurs. ●

PHOTOS DR

Un pare-feu gratuit pour se réfu

Parmi toutes les protections, si vous deviez n'en choisir qu'une, *ce serait le pare-feu, qui filtre tout ce qui rentre et sort du PC. Ici, nous allons utiliser un des pare-feu gratuits les plus efficaces, Jetico Personal Firewall. Pas facile à configurer, il est pourtant très utile, surtout avec Windows XP SP2, qui en contient un, mais très incomplet. En revanche, sous Vista, un pare-feu complet est fourni, pas des plus efficaces mais assurant tout de même une protection intéressante.* • **L.D.**



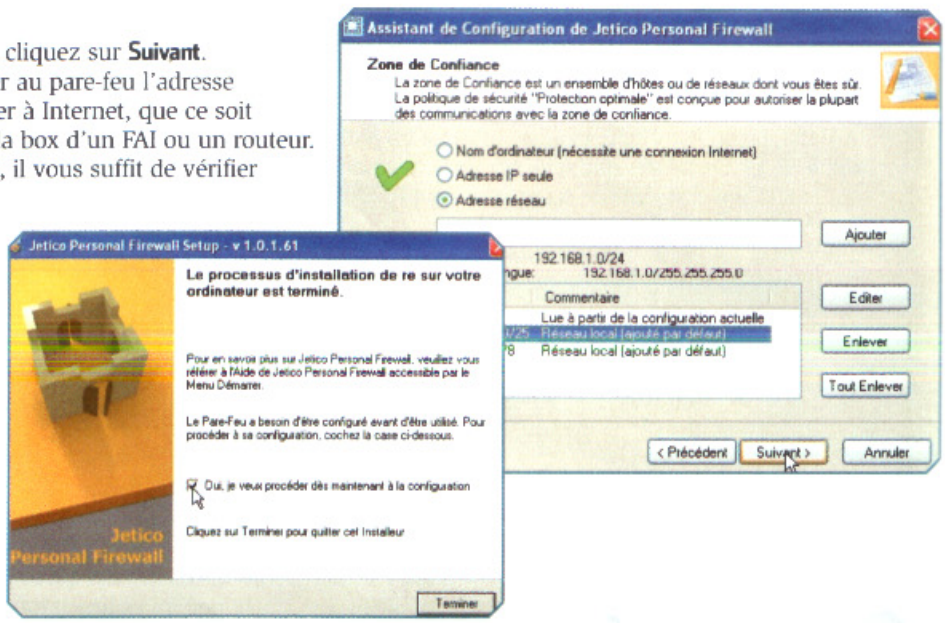


1 LES PRÉLIMINAIRES ET L'INSTALLATION

Jetico Personal Firewall est en anglais, mais il existe une traduction française que l'on peut télécharger à l'adresse **www.trad-fr.com/telecharger/details .php?file=6**. Cliquez sur **Télécharger (2,36 Mo)**. Avant de passer à l'installation, arrêtez le pare-feu de Windows XP SP2. Cumuler les pare-feu n'a pas d'intérêt, ils pourraient même entrer en conflit et ralentir le PC. Pour cela, cliquez sur **Démarrer, Panneau de configuration, Pare-feu Windows**, cochez **Désactivé** et cliquez sur **OK**. L'ordinateur va vous dire que vous courez un risque, mais ne vous en inquiétez pas trop, cela ne va pas durer. Pour lancer l'installation du nouveau pare-feu, double-cliquez sur l'icône téléchargée **Jetico_Personal_Firewall [...]**. Suivez la procédure très simple, jusqu'ici tout va bien. Les choses vont se compliquer à présent. À la fin de l'installation, cochez **Oui, je veux procéder dès maintenant à la configuration** et cliquez sur **Terminer**.

2 PRÉRÉGLER LE PARE-FEU

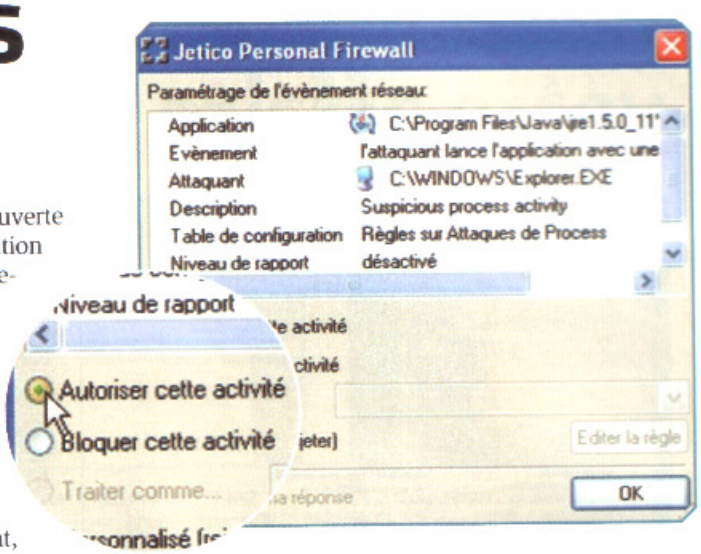
L'assistant de configuration se lance, cliquez sur **Suivant**. La première étape consiste à indiquer au pare-feu l'adresse que vous utilisez pour vous connecter à Internet, que ce soit directement avec un modem ou via la box d'un FAI ou un routeur. La fenêtre apparue semble compliquée. En fait, il vous suffit de vérifier dans l'encadré du bas que le logiciel a bien reconnu des adresses et que ces dernières sont suivies d'un **"/"** et d'un **nombre**. S'il y a un problème de reconnaissance de ces adresses IP, il vous faudra identifier votre adresse IP vous-même et la taper dans le champ de saisie suivie de /24, puis cliquer sur **Ajouter**. Cliquez sur **Suivant** deux fois (ne vous inquiétez pas de la croix rouge apparue), **Terminer**. Le logiciel vous demande alors de redémarrer l'ordinateur pour finaliser l'installation, cliquez sur **Oui** deux fois. Une fois la machine rallumée, il est possible que le logiciel vous demande d'effectuer encore un redémarrage.



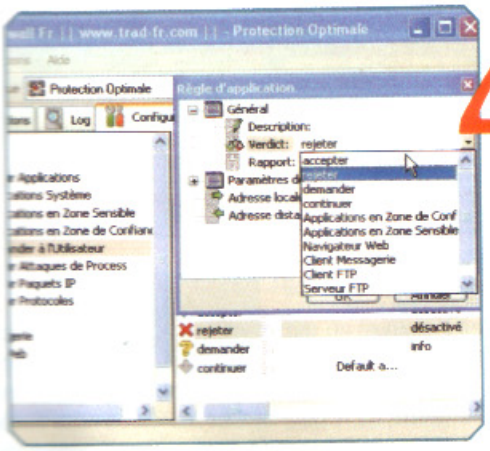
ier dans ses murs

3 LES PREMIÈRES ALERTES DE JETICO

Lorsque l'ordinateur redémarre, la fenêtre de Jetico est ouverte et l'icône du logiciel est apparue dans la zone de notification (les deux petites flèches vers le haut et le bas). Normalement, plusieurs alertes vont également surgir à l'écran. Le logiciel commence à filtrer les connexions entrantes et sortantes et à les bloquer pour savoir si elles sont dangereuses ou non. Basez-vous sur la ligne **Application**. Si vous reconnaissez le logiciel concerné, cochez **Autoriser cette activité** ; laissez coché **Enregistrer ma réponse** et cliquez sur **OK**. Si vous avez un doute, cochez **Bloquer cette activité**, décochez **Enregistrer ma réponse**, et cliquez sur **OK**. Utilisez alors vos antispywares et antivirus afin de vérifier qu'il n'y a pas de menace sur votre ordinateur. Soyez patient, de nombreuses fenêtres s'ouvriront chaque fois que vous manipulerez le PC. Peu à peu, celles-ci se feront moins nombreuses.

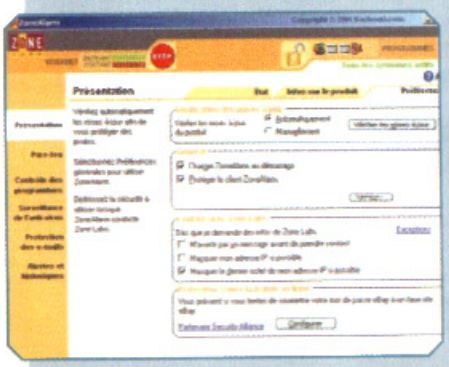


4 EN CAS D'ERREUR

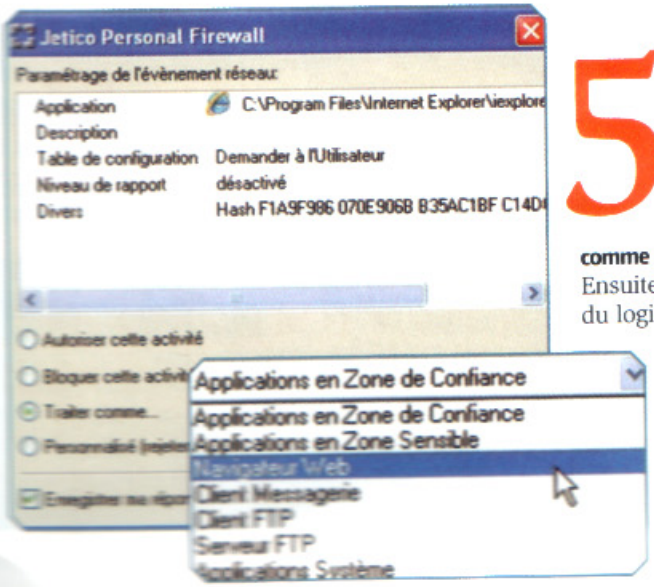


Si, au cours de l'étape 3, vous bloquez par erreur un logiciel dont vous auriez dû autoriser l'activité, vous ne pourrez plus vous en servir. Pas de panique. Si ce n'est déjà fait, ouvrez l'interface de Jetico, d'un double clic sur l'icône du logiciel dans la zone de notification. Cliquez ensuite sur l'onglet **Configuration** ; d'un clic sur le **+**, développez **Racine, Règles sur Applications, Demander à l'utilisateur**. Les applications bloquées sont marquées d'une croix rouge. Double-cliquez sur la **ligne du logiciel à débloquer** et, dans **Verdict**, choisissez **Accepter**. Le logiciel sera maintenant débloqué.

Un pare-feu plus simple à maîtriser



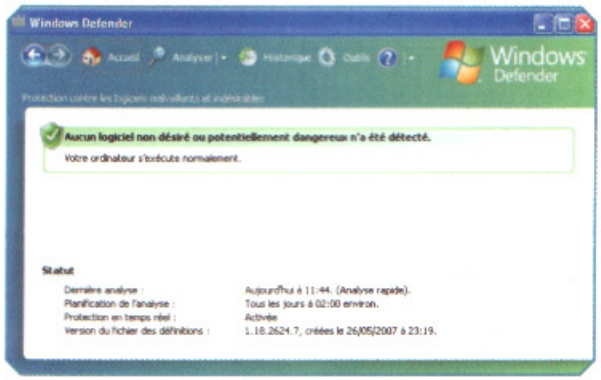
Si Jetico ne vous convient pas, tournez-vous vers un autre pare-feu, un peu moins efficace mais plus clair, par exemple ZoneAlarm. Vous pouvez le télécharger sur www.zonealarm.com. Cliquez sur **Particuliers et bureaux à domicile** ; ensuite, cliquez **sous version gratuite de ZoneAlarm** tout en bas, puis sur **Télécharger** sous ZoneAlarm Firewall. Comme Jetico, le logiciel demandera une phase d'apprentissage où vous devrez autoriser ou bloquer des logiciels. Que ce soit avec Jetico ou ZoneAlarm, si une manipulation bloque votre PC, dans le pire des cas il vous suffira de désinstaller le programme pour tout remettre en ordre.



5 LES AUTORISATIONS SPÉCIALES

Pour certains logiciels, bloquer ou autoriser n'est pas suffisant : ils peuvent répondre à plusieurs règles. C'est le cas, par exemple, d'un navigateur, d'une messagerie, d'un client FTP… Lorsqu'une demande d'autorisation concerne ce type de logiciel, cochez **Traiter comme** et, dans la liste déroulante, sélectionnez le **type d'application concernée**. Ensuite, il va falloir aller gérer ces applications spécifiques dans l'interface du logiciel. Cliquez sur l'onglet **Configuration**, développez **Racine, Règles sur Applications, Demander à l'Utilisateur pour configurer les règles du Navigateur Web**, ou bien, directement sous Racine, accédez aux **réglages du Client FTP, Client Messagerie ou Serveur FTP**. Pour éditer une nouvelle règle, cliquez droit sur un espace libre de la partie droite et sélectionnez **New, Règles d'application**. Dans la rubrique **Générale**, autorisez alors des événements. Cette partie risque de vous faire tâtonner un petit peu, mais avec l'habitude, ce sera plus simple.

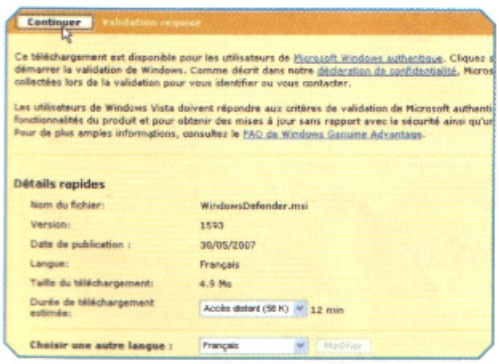
Le contre-espionnage, c'est votre affaire aussi !



Alerte aux spywares ! *Ces logiciels "espions" observent vos habitudes pour vous adresser de la publicité et, dans le pire des cas, vous voler des données personnelles. La menace vaut de se tourner vers un logiciel dédié, comme Windows Defender, fourni avec Vista (voir Panneau de configuration) ou téléchargeable pour XP, du moins si vous possédez une version légale de ce système d'exploitation.* • L.D.

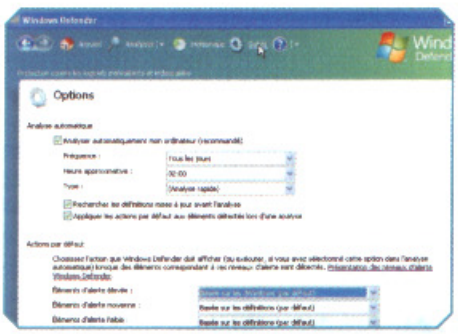
1 TÉLÉCHARGER WINDOWS DEFENDER

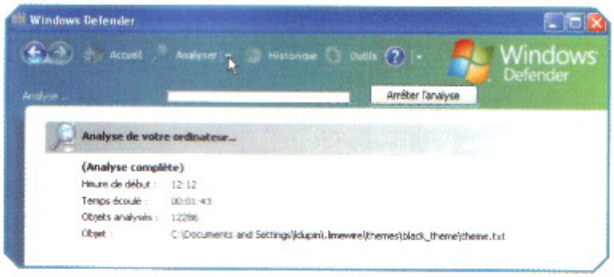
Si vous tournez sous Windows XP, vous devez télécharger Windows Defender en ligne. Pour cela, rendez-vous sur **www.microsoft.com/france/athome/security/spyware/software/default.mspx**. Cliquez sur **Téléchargez-le ici**. Fenêtre suivante, en bas de l'encadré jaune, sélectionnez **French** dans la liste déroulante et cliquez sur **Change**. Ensuite, cliquez en haut sur **Continuer**, puis sur **Télécharger (4,93 Mo)**. Double-cliquez maintenant sur **Windows Defender.msi** pour lancer l'installation. Dans la fenêtre **"Permet de protéger Windows"**, cochez **Utiliser les paramètres recommandés**, cliquez sur **Suivant** et suivez simplement la procédure.



2 CONFIGURER WINDOWS DEFENDER

À la fin de l'installation, Windows Defender effectue immédiatement une mise à jour, puis lance une analyse. Sans intervention de votre part, le logiciel est déjà apte à protéger en temps réel votre machine. Cependant, soit parce que vous vous y connaissez, soit en vous familiarisant avec le logiciel, vous aurez peut-être envie de configurer Defender à votre main. Pour cela, cliquez sur **Outils, Options**. Cela vous ouvre l'accès aux paramétrages. Notamment, descendez à la rubrique **Options de protection en temps réel**, c'est ici que vous choisirez le comportement du logiciel pour la protection permanente.





3 LANCER UNE ANALYSE À LA MAIN

Outre l'analyse en temps réel, vous pouvez lancer une analyse ponctuelle. Pour cela, dans l'interface du logiciel, cliquez sur la **flèche blanche orientée vers le bas**, à droite de Analyser. Choisissez ensuite **Analyse complète** pour fouiller les fichiers de l'ordinateur. En choisissant **Analyse personnalisée**, vous pouvez ne fouiller que des dossiers spécifiques. L'analyse se lance automatiquement. Cela peut prendre du temps si votre PC est très encombré (le nettoyer auparavant accélérera l'opération). À la fin, le logiciel vous prévient des éventuels miasmes à supprimer.

Multiplier les protections

En matière d'antispyware, il n'est pas inutile d'utiliser plusieurs logiciels en même temps. Pas forcément des logiciels d'analyse en temps réel, qui risqueraient d'alourdir votre PC, mais plutôt, en plus de Windows Defender, un logiciel d'analyse ponctuelle comme Spybot Search & Destroy, téléchargeable sur **www.safer-networking.org/fr** (4,8 Mo), ou encore Ad-Aware, à récupérer sur **www.lavasoftusa.com** (4,62 Mo). Lancer l'un de ces deux logiciels correctement mis à jour une à deux fois par mois, devrait vous protéger au mieux.

Des sites pour prendre le dessus

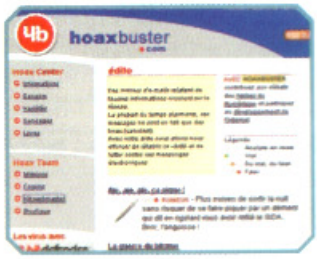
L'actu *de la sécurité*

Une des plus anciennes adresses du Web francophone en matière d'infos sur le hacking, les pirates, le téléchargement illégal et tous ces petits virus qui nous enquiquinent. Zataz suit aussi de près l'actu des "défaceurs", ces pirates qui pénètrent un site Web pour en changer le contenu.
• **www.Zataz.com**

Bonne initiative, ce portail de la sécurité informatique mis en place par les pouvoirs publics afin de protéger les internautes français du malware. On y trouve des articles de vulgarisation sous forme de blog et des outils pratiques. Dont ANSMO, un logiciel de diagnostic qui permet de faire le point sur les risques qu'encourt votre ordinateur (disponible mi-juillet)
• **www.securite-informatique.gouv.fr**

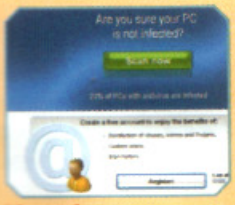
Secuser.com est une mine d'infos francophone clairement destinée aux accros à la sécurité informatique. Actualité, description des vulnérabilités connues et des nouvelles tentatives de phishing... Il y a de quoi lire et, aussi de quoi soigner son PC malade.
• **www.secuser.com**

***"La fondation Shadowserver collecte des renseignements** sur la face sombre de l'Internet".* Autrement dit sur les botnets, les virus, les attaques distribuées et toutes les menaces émergentes. Le site est en anglais, mais la section Maps (cartes), impressionnante, vaut le détour.
• **www.shadowserver.org**



Spams, légendes urbaines, rumeurs infondées : hoaxbuster s'est donné pour mission de s'attaquer à toutes ces chaînes et autres mails "à forwarder" qu'on aimerait mieux ne pas recevoir.
• **www.hoaxbuster.com /index.php**

Les outils



Vous n'avez pas d'antivirus et avez besoin d'un scan rapide de votre disque ? Utilisez donc un utilitaire en ligne. Ils sont gratuits et peuvent vous permettre de vous sortir d'un mauvais pas. Plusieurs éditeurs en proposent, comme Panda : **www.pandasecurity.com /homeusers/solutions/ activescan**

Outre un antivirus en ligne, Trend Micro fournit aussi un nouvel outil gratuit, RUBotted (encore en version bêta), capable de vous dire si votre PC a été kidnappé au sein d'un botnet. RUBotted permet également de supprimer les logiciels malveillants. **www.trendsecure.com/ portal/en-US/tools/ security_tools/rubotted**

Voilà qui est pratique pour tester un fichier qui vous paraît suspect !

Vous téléchargez Virus Total et pouvez ensuite le soumettre à votre place à l'ensemble des antivirus du marché ! Intéressante aussi, la page de statistiques qui fournit des noms et des chiffres précieux. **www.virustotal.com/fr**

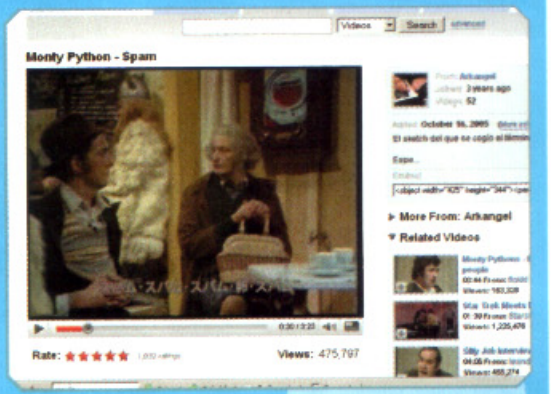
Et votre Firewall, est-il efficace ? Avez-vous des ports sensibles ouverts sur votre PC ? Pour le savoir, pratiquez check.sdv, un test de tous vos ports qui vous crée un rapport précis sur l'état de votre machine. **http://check.sdv.fr**

Marre de vous faire spammer ? Alors, utilisez un mail jetable !

Sur Jetable.org, vous avez la possibilité de créer une adresse mail temporaire que vous aurez le droit d'utiliser pendant une heure, une semaine ou un mois, à votre convenance. Tous les mails de cette fausse adresse seront routés vers votre véritable mail, jusqu'à ce qu'elle expire. **www.jetable.org**

Pour rire

Jouez au hacker quelques minutes : voilà ce que propose Isatcis, un jeu sur 16 niveaux de difficulté progressive dans lequel vous devez trouver le mot de passe pour pénétrer un (faux) système informatique. Conseil pour les grands débutants : analysez le code source des pages !
• **http://isatcis.com/**



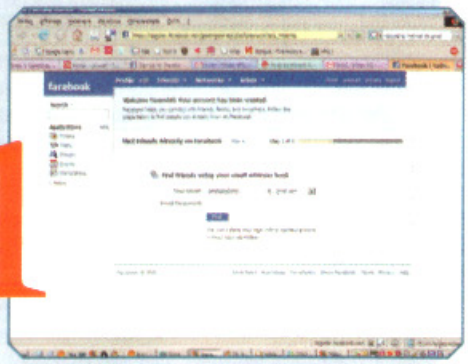
Le sketch *Spam* des Monty Python, duquel est tiré l'appellation anglaise des pourriels, est disponible sur Youtube. À le regarder, on comprend beaucoup mieux pourquoi les pionniers du Net ont ainsi baptisé les courriers publicitaires indésirables !
• **www.youtube.com/watch?v=ODshB09FQ8w**

Facebook : 10 règles

L'espace de rencontre et d'échange Facebook est un bel outil social. *Mais vos données persos ont vite fait de se retrouver en libre accès sur le réseau. Et vous pourriez être dépassé par le flot d'informations que ce site brasse autour de vous. Nos conseils pour ne pas vous perdre.*

1 MÉFIANCE À L'INSCRIPTION !

Vous venez de créer votre compte ; Facebook vous demande si vous désirez trouver des amis déjà présents sur le site par le biais du carnet d'adresses de votre webmail. Vous pouvez passer cette étape (**Passer**). Si vous acceptez d'utiliser le Friend Finder, décochez tous les contacts que vous ne souhaitez pas voir ajoutés à votre liste d'amis. Faites encore **Passer**, sinon Facebook enverra une invitation à tous les contacts sélectionnés. Vous pourrez les retrouver plus tard par le Friend Finder, depuis la page d'accueil. Ou par le biais du champ de recherche.

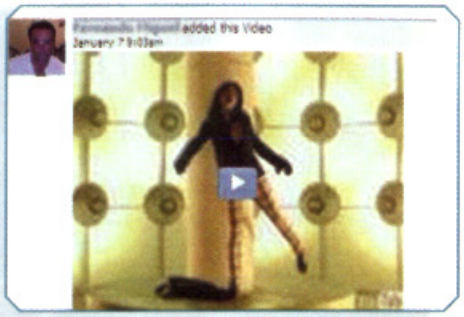


2 REMPLISSEZ VOTRE PROFIL EN CONNAISSANCE DE CAUSE

Facebook vous incite à en dire beaucoup sur vous : âge, sexe, religion ou opinions politiques. Tous ces champs sont facultatifs. Il peut être sympa de retrouver des amis d'enfance en renseignant les lycées, écoles ou universités que vous avez fréquentés. Mais prudence sur les infos trop sensibles : par défaut, tous les membres peuvent vous rechercher en fonction de l'ensemble des informations de votre profil. Il est donc déconseillé de laisser vos adresse, téléphone, voire e-mail.

3 NE FONCEZ PAS DANS LE MUR !

Il est fort possible que la première application que vous utilisiez dans Facebook soit "Le mur", espace réservé aux commentaires de vos amis (texte, liens, images, vidéos ou extraits musicaux). De nombreux utilisateurs lui préfèrent un "mur" plus complet : Super Wall ou Fun Wall (en fait des applications tierces), qui proposent d'intégrer de grandes photos ou vidéos, des dessins ou des cartes de vœux. Deux applications qui peuvent vite se transformer en réceptacle illisible qui va se remplir d'informations hétéroclites, voire de hoax ou de spam, surtout que Fun Wall comme Super Wall incitent à faire suivre (forward) les vidéos reçues... Attention aussi à ne pas répondre à tous vos amis par Forward au lieu de Reply, ce qui arrive parfois aux débutants.

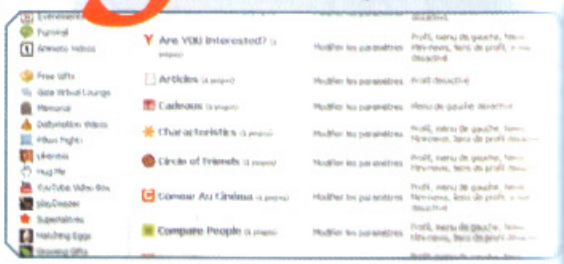


4 N'INSTALLEZ PAS LES APPLICATIONS TROP VITE...

Chaque application s'installe via une fenêtre présentant toujours les mêmes options, toutes cochées (*capture ci-dessus*). Le mieux est de tout décocher, sauf la première case, indispensable. Si vous souhaitez mettre l'application en avant, cochez **Ajouter une boîte dans mon profil** ; elle apparaîtra sur votre page. L'option "Placer un lien sous la photo..." est intrusive et inutile. Quant à "Publier des articles...", elle montre à vos amis ce que vous faites avec. Alors, gare !

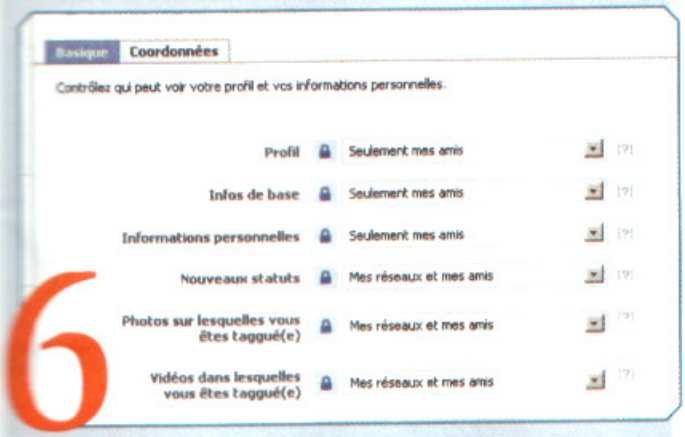
5 ... ET APPRENEZ À BIEN LES SUPPRIMER

Certaines applications deviennent parfois insupportables. Pour les supprimer, rien de plus simple : allez dans la page **Confidentialité** puis cliquez sur **Applications**. La liste des programmes tiers apparaît, et il ne reste plus qu'à cliquer sur **Supprimer** pour en retirer un de votre profil.



pour se faire respecter

6 DÉCIDEZ DE QUI VOIT QUOI



Vous n'avez peut-être pas envie de voir votre profil visité par n'importe quel membre inscrit sur Facebook. Surtout que sans intervention de votre part, tout le monde voit l'intégralité de votre profil ! Pour cela, une seule direction, la page **Confidentialité**. Cliquez d'abord sur **Profil** et choisissez si vous préférez autoriser l'accès à votre profil à vos amis (**Seulement mes amis**) ou à tous les gens des réseaux auxquels vous appartenez (**Mes réseaux et mes amis**). Vous pouvez aussi détailler dessous qui peut voir quoi, fonction par fonction. Sauvegardez et retournez ensuite dans la page **Confidentialité**, puis cliquez sur **Recherche** pour définir cette fois qui peut vous trouver dans les résultats de recherche. Par défaut, tous les utilisateurs le peuvent, mais vous pouvez, là encore, restreindre la recherche à vos amis seulement ou à un réseau en particulier. En bas de la page, vous choisirez de ne partager que certains détails sur vous si vous avez accepté d'apparaître dans les résultats de recherche.

7 GÉREZ DES REQUÊTES À LA PELLE

Un utilisateur invétéré de Facebook peut recevoir des dizaines de requêtes par jour… Pas la peine d'angoisser si l'invitation à la soirée d'un ami que vous venez de recevoir ne vous branche pas : le clic sur **Ignorer**, équivalant à un refus, n'est pas notifié au membre qui l'a envoyée. Si vous recevez décidément trop de requêtes, pensez à **Ignoreall**, un petit "bookmarklet" disponible sur www.ignoreall.com, qui supprimera d'un coup toutes les demandes qui vous ont été envoyées.

8 FUYEZ LES APPLICATIONS MALVEILLANTES

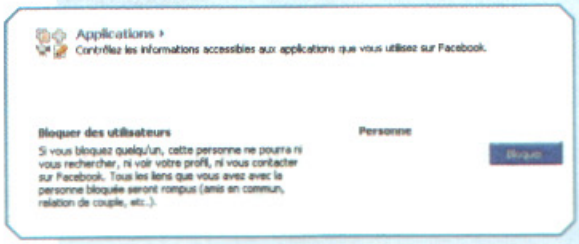
La nature virale de Facebook fait que les applications les plus courues ne sont pas forcément les meilleures. Certaines vous obligent à inviter une vingtaine d'amis avant de voir vos résultats… D'autres services indépendants vous présenteront des pseudo-nouveautés ou vous annonceront qu'un de vos amis les a utilisées. Appelons un chat un chat, tout ceci relève du spam. Pour en finir, cliquez sur **Applications** dans la colonne de gauche. Là, vous pouvez, pour chaque application, choisir comment elle interagit avec votre profil et supprimer les envois d'e-mails qu'elle effectue. Cliquez juste sur **Modifier les paramètres**. Vous pouvez aussi vous débarrasser d'un service ennuyeux et ne plus recevoir de requêtes de vos amis pour l'installer. Entrez son nom dans le champ de recherche, cliquez sur **Voir Application** sur le bon programme de la liste qui apparaît alors, puis sur **Bloquer l'application**.

9 SOURIEZ, VOUS ÊTES TAGUÉ !

Facebook dispose d'une puissante fonction de partage de photos, qui permet notamment à l'un de vos amis de vous associer à une photo… qui, du coup, sera vue par tous ses amis dans son profil ! Si vous avez été "tagué" par un ami et que le cliché ne vous convient pas, rendez-vous simplement sur la photo litigieuse et cliquez sur **Supprimer le tag**. La photo ne vous sera plus associée.

10 DÉBARRASSEZ-VOUS DES NUISIBLES

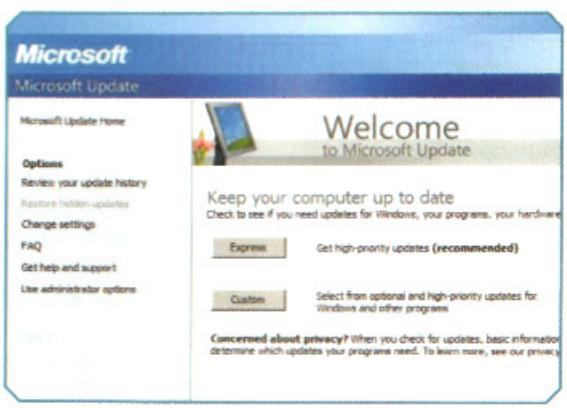
Une connaissance vous ennuie ? Vous ne voulez surtout pas retrouver une certaine personne sur Facebook ? Cliquez sur **Confidentialité** et rendez-vous tout en bas de la page, à la rubrique **Bloquer des utilisateurs**. Inscrivez simplement le nom de l'indésirable pour le mettre en quarantaine : il ne pourra plus ni vous contacter, ni voir votre profil.



Self-defense : l'antivirus ne

Une bonne "hygiène informatique" peut, la plupart du temps, *suffire à contrecarrer les plans des mafias du Web. Voici nos bons conseils pour surfer en paix.* • **Par Éric Le Bourlout**

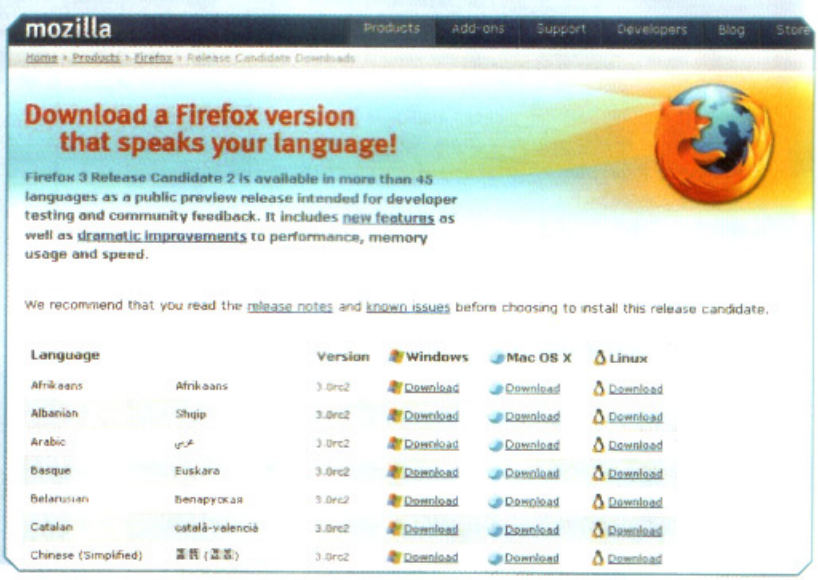
Maintenez votre système à jour



C'est la règle numéro 1 : conservez un système le plus à jour possible. Car bien des virus se propagent, en réalité, parce que des utilisateurs ont négligé de le faire. Notamment en activant les mises à jour automatiques proposées par Microsoft, qui corrige très rapidement les failles de Windows détectées. Il est de plus en plus important de mettre à jour très régulièrement les programmes tiers aussi : Flash, qui est la victime d'un virus en ce moment, ou encore Winamp ou Real Player sont des cibles de choix pour les pirates.

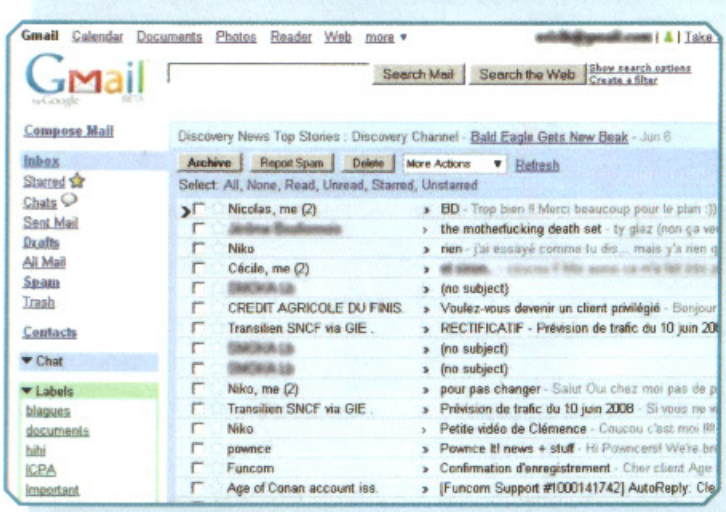
Privilégiez Firefox

Microsoft a fait d'énormes progrès en matière de sécurité avec Internet Explorer 7 (IE6 était un nid à virus dont il faut vite se débarrasser !) mais on constate tout de même que bien des attaques sont destinées exclusivement au navigateur de Microsoft. La troisième mouture de Firefox vient d'être lancée, et nous vous la recommandons chaudement, d'autant qu'elle intègre la technologie Safe Browsing de Google, qui vous prévient lorsque vous tombez sur un site de phishing ou connu pour abriter des virus.



UTILISEZ PLUSIEURS MAILS

Si vous centralisez tous vos courriers sur un même mail, il est possible qu'au bout de quelques mois, vous crouliez sous les courriers indésirables... Surtout si vous avez pour habitude de vous inscrire sur de nombreux sites. Utilisez-donc aux moins deux adresses mail : l'une d'elles servira de "poubelle" pour le tout-venant, et vous réserverez l'autre à vos amis et contacts pour une correspondance plus sérieuse ou précieuse. De même, ne laissez jamais votre adresse e-mail "en clair" sur la Toile : les spammeurs utilisent des robots qui récupèrent automatiquement les mails sur le Web.

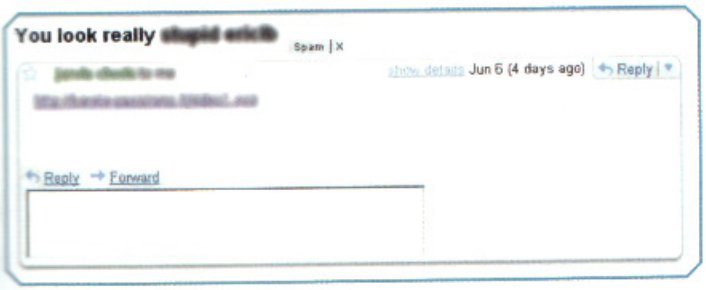


FAITES BON USAGE DE VOTRE PARE-FEU

Le pare-feu (firewall en anglais) est l'une arme de vos armes les plus puissantes pour vous défendre contre les pirates, puisque ce petit bout de programme (que l'on trouve gratuitement sur le Net, à l'instar de Zone Alarm) est capable de protéger votre ordinateur de certaines attaques en filtrant les données qui sortent de la machine ou qui y entrent. La box ADSL de votre fournisseur d'accès à Internet peut aussi remplir cet office. Quant à Windows XP et Vista, ces deux systèmes d'exploitation intègrent un pare-feu (plus complet pour Vista que pour XP) qu'il est préférable d'activer si vous n'utilisez pas un logiciel tiers.

le fait pas pour vous

Prudence en téléchargeant

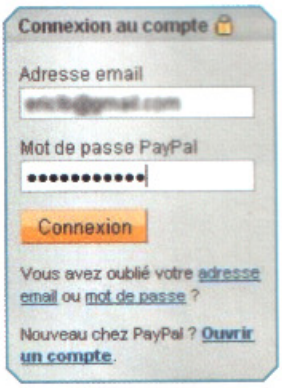


On ne le dira jamais assez : de nombreux logiciels malveillants arrivent sur un ordinateur parce que l'utilisateur a ouvert un fichier sans faire attention. Ne téléchargez surtout pas de fichiers exécutables par exemple. Evitez-les même comme la peste si vous n'avez qu'une confiance limitée dans le site depuis lequel vous le rapatriez. Idem sur les réseaux peer to peer, connus pour abriter de nombreux fichiers pourris, cachés par exemple sous le nom d'un film ou d'un jeu.

ATTENTION AUX HOT SPOTS !

Génial, de pouvoir se connecter n'importe où sur un hot spot... Mais attention, il y a des risques, tout au moins quand on se connecte à un point d'accès dont on ne connaît pas le responsable. Car il est tout à fait possible à un pirate de créer un hot spot en libre accès capable de "sniffer" les informations que vous envoyez... Voire de récupérer à la volée vos échanges entre votre machine et le point d'accès. Evitez donc de vous connecter sur des sites sensibles et d'entrer des mots de passe, car ils sont très facilement récupérables.

Changez de mot de passe !



Voilà un point très important : les internautes ont tous tendance à employer les mêmes mots de passe sur tous les services qu'ils utilisent. Ce que savent bien les cybercriminels, qui exploitent cette paresse naturelle en testant identifiants et mots de passe sur de nombeux sites, à commencer par Paypal... Changez donc de mot de passe en fonction du site et essayez d'en utiliser de plus complexes que votre date de naissance ou le nom de votre enfant, qui peuvent être facilement trouvés par le biais du "social engineering" (*voir aussi page 28*).

Vérifiez que tout est bien crypté

Détails techniques

Connexion chiffrée : chiffrement de haut niveau (RC4 128 bit)
La page que vous voyez a été chiffrée avant sa transmission sur Internet.
Le chiffrement rend très difficile aux personnes non autorisées la visualisation de la page durant son transit entre ordinateurs. Il est donc très improbable que quelqu'un puisse lire cette page durant son transit sur le réseau.

Lorsque vous entrez des informations personnelles sur un site – vos identifiants sur le site de votre banque, par exemple –, vérifiez bien que l'icône "cadenas" – en bas à droite dans Firefox et à droite de la barre d'adresse dans Internet Explorer 7 – est verrouillée. Attention, IE7 renvoie souvent des "faux positifs" en vous indiquant que le site n'est pas fiable alors qu'il l'est ! Vous pouvez aussi vérifier la confidentialité de la transmission en regardant si le début de l'adresse commence bien par "https://"

MÉFIANCE SUR MESSENGER

Windows Live Messenger est le client de messagerie instantanée le plus utilisé en France... Et aussi un vecteur fréquent de virus. Il se peut qu'un ami vous envoie des messages ou des fichiers étranges dès que vous vous connectez : surtout, ne cliquez pas dessus, ce sont des fichiers contaminés qui pollueront votre machine et se réexpédiront automatiquement à tous vos contacts lorsque vous lancerez MSN.

Gare aux amis inconnus !

Vous avez peut-être déjà reçu des mails de gens (souvent des filles) souhaitant devenir votre ami(e), et vous demandant d'ajouter son adresse sur Windows Live Messenger ou de lui répondre. Méfiance, derrière ces mails, anodins mais tentants, se cachent souvent des scammeurs qui ont pour ambition de vous mettre en confiance pour vous extorquer de l'argent ou des données personnelles.

FAITES DES SAUVEGARDES

La plupart des virus ne sont plus destructeurs, mais il y a toujours un risque d'y perdre ses données. Pour preuve, un virus se balade actuellement sur le réseau, qui crypte vos données et vous demande de l'argent pour obtenir un code de décryptage ! Alors pour éviter tout cela, mieux vaut faire des sauvegardes régulières de toutes vos données personnelles, et utiliser pour plus de sécurité un logiciel d'image disque (de type Norton Ghost) dès que votre système est installé, pour être en mesure de le réinstaller en quelques minutes en cas de malheur.

Vidéo

LA TRILOGIE MATRIX

Les films d'Andy et Larry Wachowski racontent l'histoire de Neo (Keanu Reeves), un employé de bureau qui vit dans la Matrice, un monde fictionnel simulant la fin du vingtième siècle, créé de toutes pièces par des machines pour asservir l'humanité. Neo est "réveillé" par Trinity et Morpheus, deux hackers capables de passer de l'apocalyptique monde réel à la Matrice en piratant des lignes utilisées par les machines. Vanté à l'époque pour ses effets spéciaux détonants, Matrix est aussi un bel hommage à la culture hacker. Trinity emploie d'ailleurs de vraies commandes Unix, dont un hack connu, dans les différents films.

GHOST IN THE SHELL

Cette série de mangas, puis d'*anime* cyberpunk créée par Masamune Shirow – qui inspira Matrix – est située dans un Japon futuriste dans lequel humains et cyborgs cohabitent. On suit les aventures de Motoko Kusanagi, cyborg policière spécialisée dans le cybercrime. Dans le premier film, elle cherche à retrouver le Puppet Master, un mystérieux hacker capable de pirater les cerveaux pour faire des pantins de ses victimes. Une nouvelle adaptation au cinéma, produite par Dreamworks, devrait voir le jour cette année.

DIE HARD 4 *RETOUR EN ENFER*

John McClane reprend du service et dans cet épisode va avoir affaire à de nouveaux gros méchants : des cyberterroristes, avec à leur tête un hacker des plus doués, Thomas Gabriel. Avec l'aide de quelques pirates informatiques, Gabriel parvient à faire tomber les réseaux informatiques qui contrôlent les communications, l'électricité et même la Bourse, ce qui provoque une bien jolie panique dans les rues de New York ! C'est complètement exagéré – pirater un satellite avec un téléphone mobile ne doit pas être évident – mais on s'amuse bien.

CULTURE

WARGAMES

David Lightman est un pirate informatique adolescent qui croit avoir trouvé une "backdoor" vers un serveur lui proposant de nouveaux jeux. En fait, il vient d'entrer sur un ordinateur militaire… Et débute une partie de "guerre thermonucléaire globale" entre les USA et la Russie. Est-ce un jeu, est-ce la réalité ? Le film a bien vieilli, ordinateurs et consoles de jeux paraissent tout droit sortis de la préhistoire de l'informatique. Mais *Wargames* est l'un des tout premiers films à avoir mis un hacker en vedette et reste, à ce titre, un must de la culture pirate.

CYBERTRAQUE

Adaptation du livre *Takedown* de John Markoff et Tsutomu Shimomura, ce film raconte les exploits d'un certain Kevin Mitnick (*voir nos portraits page 14*). Le film est loin d'être parfait, d'ailleurs Mitnick a indiqué qu'il comprenait de grossières erreurs. Il faut dire que c'est précisément Tsutomu Shimomura qui est parvenu à le piéger… Il demeure cependant une excellente illustration des techniques d'ingénierie sociale chères au plus célèbre des pirates informatiques.

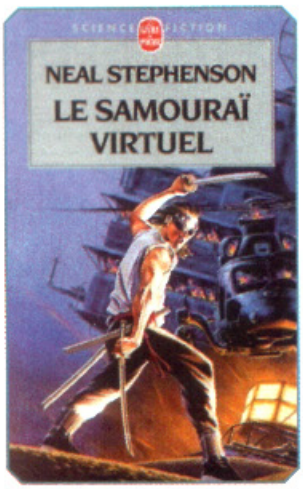
Livres

NEUROMANCIEN

Attention, livre culte ! *Neuromancien* de William Gibson est, avec la nouvelle *Johnny Mnemonic* (du même auteur), le texte fondateur du mouvement cyberpunk, qui inspira bien des mangas et films plus tard. Publié en 1984, ce roman obscur met en scène Case, un pirate informatique (appelés CowBoys) dont la connexion au cyberespace à été coupée par son employeur, qu'il avait essayé de voler. Tandis que Case erre dans les rues de la Conurb à la recherche d'une clinique qui pourrait réparer son système nerveux, il tombe sur deux personnages mystérieux qui lui proposent de lui redonner accès au cyberespace, à condition qu'il accepte un piratage fort dangereux…

LE SAMOURAÏ VIRTUEL

Hiro est un livreur de pizza sans argent dans le monde réel, mais aussi un hacker et une star du Metavers, un univers virtuel en 3D dans lequel son avatar est une véritable star, puisqu'il en a écrit une bonne partie du code. Avec son amie Y.T, Hiro découvre une nouvelle drogue, le Snow Crash, capable d'agir dans le monde réel comme dans le Metavers, sous la forme d'un virus. Il utilise alors ses dons de pirate pour enquêter sur le Snow Crash. Ce roman de Neal Stephenson, d'une imagination foisonnante, a marqué bien des esprits : il est notamment à l'origine de l'utilisation du terme "avatar" pour désigner le représentant virtuel d'une personne sur Internet.



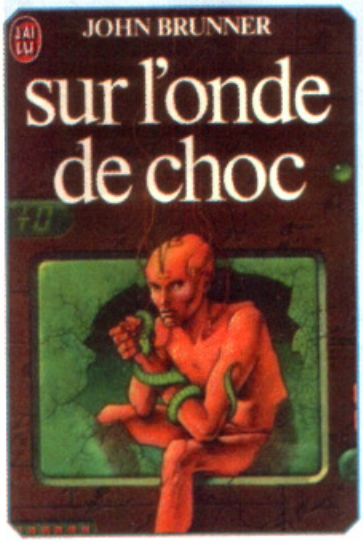
PIRATE

• Par Éric Le Bourlout

LES MAILLES DU RÉSEAU

Au même titre que William Gibson, Bruce Sterling fait partie des fondateurs du cyberpunk, et *Les mailles du réseau* est un roman phare de cette littérature… En 2020, les corporations ont remplacé les Nations ; ceux qui refusent ce nouvel ordre sont devenus des "États-pirates", qui ont légalisé le piratage de données informatiques. Le livre, écrit en 1988, décrit un monde futuriste incroyablement détaillé… Et si certains concepts ont vieilli, le "Net" qu'il met en scène rappelle en bien des points celui que nous utilisons aujourd'hui.

SUR L'ONDE DE CHOC



Ce roman, paru en 1975 est parfois considéré comme la première œuvre cyberpunk, avant même *Johnny Mnemonic*. L'action se situe au XXIe siècle. Le héros, Nick Haflinger, est un génie que l'État américain a très tôt enfermé dans une institution spécialisée pour l'étudier. Il parvient à s'enfuir et pirate ensuite identité sur identité en s'introduisant dans des systèmes informatiques afin d'échapper aux poursuites. Dans ce livre, John Brunner invente la notion de ver de réseau (worm), capable de se propager d'une machine à l'autre. Ça vous rappelle quelque chose ?

RESET

Des joueurs d'un jeu en ligne, Dystopia, ultraréaliste et organisé en réseau local au sein d'une cité, changent de personnalité, puis se suicident quand ils reçoivent le message *"Votre vie est un échec. Appuyez sur reset."* Une policière et un hacker vont enquêter et remonter la piste de l'organisateur de ce jeu morbide. Un manga en un seul volume de Tetsuya Tsutsui.

Le meilleur du spam et

« Back to Inbox | Archive | Report Spam | Delete | More Actions

Mettez fin au spam non désiré, aux pop-ups et autres dangers de l'internet DE FAÇON PERMANENTE.
Cliquez ici

SI CELA POUVAIT METTRE FIN À CE GENRE DE PUB...

« Back to Inbox | Archive | Report Spam | Delete | More Actions

From: Frank Young <xxxxx@xxxxxx.com>
To: xxxxx@xxxxxx.com
Subject: Voyageurs dans le temps, aidez-moi !!!!!
Date: 10 Jan 2002 20:43:53 +0100
Si vous êtes un voyageur dans le temps ou un extraterrestre déguisé en humain et/ou avez la technologie pour voyager physiquement dans le temps, j'ai besoin de votre aide !
Ma vie a été trafiquée et maudite !
J'ai souffert énormément et maintenant, je suis en train de mourir !
Je dois être en mesure :
- de remonter dans le temps
- de rembobiner ma vie jusqu'à l'âge de 4 ans
- d'être capable de me rappeler ce que je sais de façon à ce que je puisse empêcher ma vie d'être maudite de nouveau.
Je suis en très grand danger et j'ai besoin de ce que je demande immédiatement !
Je suis au courant qu'il existe plusieurs types de voyages dans le temps, et que les humains ne se débrouillent pas bien avec certains.
Je veux un voyage aussi proche du retour temporel que possible, aussi sûr que possible. Et remonter le temps de façon à ce que l'univers actuel cesse d'exister.
Je sais qu'il existe des gens très puissants par ici avec de l'équipement gouvernemental ou extraterrestre capables de faire cela.
Si vous pouvez m'aider, je paierai pour votre téléportation ou votre voyage ici. Ainsi que votre hôtel, votre nourriture et toutes vos dépenses. Je paierai bien pour cet équipement. La preuve de son fonctionnement doit être fournie.
Aussi, si vous êtes l'un des rares êtres à avoir la possibilité d'éditer l'univers, MERCI DE RÉPONDRE !
Si vous disposez de cette technologie et pouvez m'aider envoyez moi un mail (SÉPARÉ) à
xxxxxx@aol.com
Ne répondez pas si vous êtes un méchant extraterrestre !
Merci

EH, ÇA TE DIRAIT UN VOYAGE AU PRÉCAMBRIEN ?

« Back to Inbox | Archive | Report Spam | Delete | More Actions

Bonjour mon ami ! Je suis prêt à me suicider et à manger mon chien si le prix des médicaments sur www.coursedevelxx.com est trop cher. Regarde le site et appelle-moi au 1-800 si j'ai tort. Mon chien et moi sommes toujours en vie :-)

JE CROIS QUE JE VAIS PLUTÔT APPELER TON CHIEN.

du scam

« Back to Inbox | Archive | Report Spam | Delete | More Actions

En V.O.

A votre attention Mme et Mr.

Je me nomme cherita bana je suis secretaire de direction à la societe peugeot france .j'ai une offre pour vous. Notre societe vient de lancer un offre ou on te remettra un vehicule peugeot pour que tu fasse la pub en le roulant dans ton pays et tu sera beneficiere apres l'avoir prise.Mais il y a des dossiers à fournir comme:

1:une copie de ton permis de conduire
2:une copie de ta carte d'identite
3:ton adresse complete
4:votre passport
5: votre telephone direct

Tous les dossiers demandé doivent etre scanner et envoyer à la societe sur : societepeujot_paris_france@yahoo.fr si cette offre t'interesse contacte la societe tous de suite pour deposer ton dossier.
Mais tu peux m'ecrire quand tu voudras sur bencherita_bana@yahoo.fr ,et aussi
l'offre est limitée parce que nous recherchons 50 pays des 4 continents du monde.

Bonne comprehension

BEN, C'EST SYMPA, MAIS MOI, JE SUIS PLUTÔT RENAULT

« Back to Inbox | Archive | Report Spam | Delete | More Actions

Je suis désolé pour toi, mais ta vie va prendre fin si tu ne fais pas ce que je demande. J'ai été payé pour t'éliminer et je dois le faire dans les dix jours.
Quelqu'un que tu appelles ton ami veut te tuer par tous les moyens, et cette personne a dépensé beaucoup d'argent pour ce faire. Elle nous a donné ton nom, ta photo et toutes les informations dont nous avions besoin. Si tu as des doutes là-dessus, je t'enverrai ton nom et ton adresse dans mon prochain mail.
Pendant ce temps, j'ai envoyé mes gars pour te surveiller et ils m'ont donné tous les détails nécessaires à l'opération, mais je leur ai demandé de ne pas attaquer immédiatement car j'ai de la sympathie pour toi.
Alors, veux-tu VIVRE OU MOURIR ? À toi de décider. Reviens vers moi si tu es prêt à faire un deal, qui sait, je pourrais bien t'épargner. Tu dois juste dépenser 8 000 $. D'abord tu paies 3 500 $ et je t'enverrai une vidéo de la personne qui veut te voir mort. Quand tu auras cette vidéo, tu paieras le reste, soit 4 500 $. Si tu ne veux pas m'aider, je n'aurai d'autre choix que de poursuivre la mission pour laquelle j'ai déjà été payé.

Avertissement : ne pense même pas à appeler la police ou qui que ce soit parce que j'étendrai alors ma mission aux membres de ta famille, car la personne qui veut te tuer connait aussi ta famille.

DÉSOLÉ, MAIS ÇA SERAIT PAS COOL POUR MON AMI

« Back to Inbox | Archive | Report Spam | D

From:
parallels44@oralhealthproducts.com
Subject: best
Date: May 26, 2008 11:28:05 AM EDT
Ta vie, c'est de la merde.

OUI, MAIS QU'EST-CE QUE JE DOIS FAIRE ?

« Back to Inbox | Archive | Report Spam | D

Vous êtes invités à faire du shopping sur une large sélection de bombes et de roquettes sol-air, sol-sol, et d'armement disponible a prix réduit. Avec ces roquettes vous pourrez commettre des attaques terroristes, détruire des bâtiments, des stations électriques, des ponts, des usines et tout ce qui vous vient d'autre à l'esprit. La plupart des articles sont en stock et disponibles pour livraison le jour suivant aux USA. Une livraison internationale est disponible avec un coût supplémentaire. Les prix sont négociables.
Contactez-nous par ICQ #123456798 ou directement par téléphone au +1 234 657 145
L' offre du jour :
******* BOMBES *******
Bombe à fragmentation OFAB-500U HE
Bombe FAE - Pas en stock
Bombe perce-béton BETAB-500U

ON VOUS RASSURE, CE SPAM EST UN HOAX !

• Traduit de l'anglais par Éric Le Bourlout

Quiz spécial sécurité

Testez vos connaissances en sécurité informatique *grâce à ce petit quiz. C'est facile puisque toutes les réponses sont dans ce magazine ! Sauf, bien sûr, si vous avez commencé par la fin...*

• par Éric Le Bourlout

1 En quelle année est apparu le premier virus pour compatibles IBM PC ?
a - 1975
b - 1982
c - 1986

2 Qui a pour la première fois employé le terme "virus" dans un contexte informatique ?
a - Fred Cohen
b - John Von Neumann
c - Peter Norton

3 Quelle est la particularité du "worm" ?
a - Il se réplique sur le disque dur de l'ordinateur
b - Il est capable de détruire des données sur votre disque
c - Il se propage par le réseau

4 Qui a créé le premier virus de macro ?
a - Le Russian Business Network (la cybermafia russe)
b - Un employé de Microsoft
c - Remi Celgan, un adolescent de 15 ans

5 Qu'est ce qu'un botnet ?
a - Un réseau de PC piratés
b - Un logiciel peer-to-peer pour les pirates de contenus
c - Un robot de conversation qui envoie du spam par messagerie instantanée

6 Que surveille un firewall ?
a - Les fichiers exécutables que vous téléchargez
b - Les paquets de données qui circulent entre votre ordinateur et Internet
c - La présence de spywares et d'adwares sur votre ordinateur

7 Pourquoi surnomme-t-on l'arnaque à l'africaine "scam 419" ?
a - À cause de l'erreur HTTP 419, qui signifie "accès refusé"
b - À cause de la directive 419, qui protège les Américains contre ces arnaques
c - À cause de la loi nigériane 4.1.9, qui interdit cette pratique

8 De quoi le tout premier spam faisait-il la promotion ?
a - D'un ordinateur
b - D'un forum pornographique
c - D'un logiciel de traitement de texte

9 Qu'est ce que Rock Phish ?
a - Un filtre antiphishing
b - Le groupe de rock qui a donné son nom au phishing
c - Un logiciel pour faciliter le travail des "phisheurs"

10 Quel est le principal fait d'armes de Jon Lech Johansen ?
a - Il a réussi à pirater les lignes téléphoniques de l'opérateur américain Bell.
b - Il a fait virer plusieurs millions de dollars vers plusieurs comptes de par le monde.
c - Il a cassé la protection des DVD vidéo.

Vous avez de 0 à 5 réponses justes : Eh bien, on dirait que quelques révisions s'imposent ! Si vous avez séché sur les questions liées à la sécurité de votre ordinateur, refaites un petit tour dans le magazine que vous tenez entre les mains, notamment nos conseils pratiques (*pages 54 à 63*).

Vous avez de 6 à 10 bonnes réponses : Bravo ! Les hackers, virus et autres cyber-arnaques ne semblent plus avoir trop de secrets pour vous. Mais méfiance, on n'est jamais trop prudent, d'autant que de nouvelles menaces débarquent chaque jour. Restez sur vos gardes !

RÉPONSES

1-c ; 2-a ; 3-c ; 4-b ; 5-a ; 6-b ; 7-c ; 8-a ; 9-c ; 10-c

ABONNEZ-VOUS à notre offre privilège

1 an d'abonnement à SVM (soit 11 n°)

les 6 hors-séries SVM 2008

soit 4 SVM "Pratique"
+ 2 SVM "Les Grands Dossiers"

SVM " Pratique "
Encore plus de conseils pratiques pour décrypter, comprendre et maîtriser sa micro

SVM " Les grands dossiers "
Véritable collection de prestige du magazine qui a pour vocation de traiter les sujets forts d'actualité et d'aller plus loin sur les thèmes high-tech et scientifiques du moment

=

49€

seulement
au lieu de ~~70,95€~~*

Collection complète SVM

soit 30% d'économie

Bulletin d'abonnement

A remplir et à retourner avec votre règlement sous enveloppe non-affranchie à : **SVM • Libre réponse 38081 • 75919 Paris Cedex 19**

☐ **OUI,** je m'abonne à SVM
pour 1 an (11 n°) + 6 hors-séries au prix de 49€ seulement au lieu de 70,95€* soit une économie de 30%

☐ **OUI,** je souhaite recevoir la newsletter hebdomadaire de SVM et j'indique ci-contre mon adresse e-mail.

Je joins à présent mon réglement

☐ par chèque à l'ordre de SVM
☐ par Carte Bancaire
expire fin
Date et signature obligatoires :

HS05

J'indique ici mes coordonnées : M. ☐ Mme ☐ Mlle ☐

Société
Nom
Prénom
Adresse
Code postal Ville
Tél. : Fax :
E-mail : @

☐ J'accepte d'être informé(e) par e-mail des offres commerciales du groupe Volnay Publication et de celles de ses partenaires.

* Prix de vente des magazines chez votre marchand de journaux (46,75€) + 4 SVM " Pratique " (15,20€) + 2 SVM " Les grands dossiers " (9€). Offre non remboursable. Dans la limite des stocks disponibles. La TVA de 2,10% sur l'abonnement est incluse.
Pour les tarifs étrangers ou toute autre demande, merci de nous consulter au 01 44 84 80 26.
Conformément à la Loi Informatique et Liberté du 06 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant. Si vous ne souhaitez pas recevoir de sollicitations commerciales et/ou études, il vous suffit de bien vouloir nous en informer.
Date limite de validité : 31/12/08

Volnay Publication France - 34, rue Jean Jaurès - 92808 Puteaux - SAS au capital de 7 308 280 € - RCS Paris 494 165 665 00014
Service Abonnements - Tél. : 01 44 84 80 26 - Fax : 01 42 00 56 92 - svmabo@dipinfo.fr

Retrouvez toutes nos offres sur : www.volnaylekiosque.fr

NETGEAR®

Connect with Innovation™

Internet partout chez vous, **simplement** et **rapidement** via les prises électriques

- **Aucune installation logicielle nécessaire !**
- Transformez n'importe laquelle de vos prises électriques en une connexion réseau
- Connectez simplement des PC, votre Décodeur TV ADSL, des platines réseau multimédia, des PlayStation 3™ ou encore des X-Box 360™ sur votre réseau
- Compatible Windows Vista et Mac®

POWERLINE 85 Mbps

Pour un accès internet et de la messagerie

CPL 85Mbit/s

Unitaire - XET1001

Pack de 2 - XETB1001

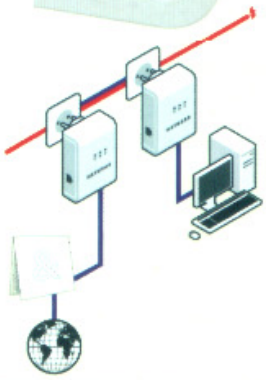
POWERLINE HD 200 Mbps

Pour une utilisation multimédia intensive (jeux, vidéo...)

CPL 200Mbit/s

Unitaire - HDX101

Pack de 2 - HDXB101



A partir de 54,90 €TTC

WWW.NETGEAR.FR

Toutes les marques ou noms de produits cités sont la propriété de leur détenteurs respectifs.